

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, (b) (6)

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)
)
)
)
)
)
)
)
)
)
)

**DEFENSE MOTION FOR
JUDICIAL NOTICE OF
H.R. 553 AND CONGRESSIONAL
HEARINGS DISCUSSING
CLASSIFICATION**

DATED: 16 November 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, moves this court, pursuant to Military Rules of Evidence (M.R.E.) 201, 201A, and 803(8) to take judicial notice of H.R. 553, the "Reducing Over-Classification Act," and transcripts of House Committee meetings on the Espionage Act (16 December 2010) and Over-Classification (22 March, 26 April, and 28 June, 2007).

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting Government property, and two specifications of knowingly exceeding authorized access to a Government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were referred to a general court-martial on 3 February 2012.

5. On 7 October 2010 President Barack Obama signed H.R. 553, also known as the "Reducing Over-Classification Act." See Attachment A.

6. The law, which requires “the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information,” included a number of findings. *See* Attachment B. The law’s findings include:

a. The National Commission on Terrorist Attacks Upon the United States (commonly known as the ‘9/11 Commission’) concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies. *Id.*

b. The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information. *Id.*

c. Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector. *Id.*

7. On 16 December 2010, Thomas Blanton, Director of the National Security Archive at George Washington University testified before the House’s Committee on the Judiciary during a hearing on the Espionage Act and the constitutional implications of WikiLeaks. *See* Attachment C. Mr. Blanton testified that 50-90% of what is classified is either over-classified or should not be classified at all. *Id.* He further testified that over-reaction to leaks is well-documented throughout American history. *Id.*

8. Over the course of three days in 2007 (22 March, 26 April, and 28 June) the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the House Committee on Homeland Security heard testimony on Over-Classification and Pseudo-Classification. *See* Attachment D. The hearings include testimony from a number of public officials and experts discussing the negative impact of over-classification and the problems presented by the practice. *Id.*

WITNESSES/EVIDENCE

9. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this Court to consider the referenced attachments to this motion in support of its request.

LEGAL AUTHORITY AND ARGUMENT

10. In the interest of judicial economy, M.R.E. 201(a) and 201A relieve a proponent from formally proving certain facts that reasonable persons would not dispute. First, the military judge may take judicial notice of adjudicative facts “capable of accurate and ready determination

by resort to sources whose accuracy cannot reasonably be questioned.” M.R.E. 201(b)(2). This category of adjudicative facts includes government records, business records, information in almanacs, scientific facts, and well documented reports. *Id.* See also, *United States v. Spann*, 24 M.J. 508 (A.F.C.M.R. 1987). The key requirement for judicial notice under this category is that the source relied upon must be reliable. Pursuant to M.R.E. 201A, a military judge, “may take judicial notice of domestic law.”

11. Under M.R.E. 201(d), a military judge must take judicial notice if the proponent presents the necessary supporting information. In making the determination whether a fact is capable of being judicially noticed, the military judge is not bound by the rules of evidence. 1 STEPHEN A. SALTZBURG, LEE D. SCHINASI, AND DAVID A. SCHLUETER, *MILITARY RULES OF EVIDENCE MANUAL* 201.02[3] (2003). Additionally, the information relied upon by the party requesting judicial notice need not be otherwise admissible. *Id.* The determination of whether a fact is capable of being judicially noticed is a preliminary question for the military judge. See M.R.E. 104(a).

12. H.R. 553 is appropriate for judicial notice. As a bill that was signed into law by the President of the United States, it unquestionably qualifies as domestic law as contemplated by M.R.E. 201A. Because the “Reducing Over-classification Act” is a domestic law it is appropriate for judicial notice. M.R.E. 201A. Likewise, the law is relevant on both the merits and sentencing. Congress found that overclassification results in confusion about what information can be shared with whom. See Attachment B. This fact would rebut any argument that PFC Manning had a reason to know that information could be used to the injury of the United States or to the advantage of a foreign nation simply because a document is classified. See Amicus Curiae Brief of Pepperdine University School of Law, *United States v. Diaz*, 2010 WL 519394. Because H.R. 553 makes an element of several Specifications less likely it is relevant on the merits.

13. The law would also be relevant during any pre-sentencing phase of PFC Manning’s trial. R.C.M. 1001(c) permits an accused to present matters in extenuation and mitigation during such a phase. These matters would tend to explain the circumstances surrounding the commission of an offense or tend to lessen the punishment. *Id.* The acknowledgment by Congress that PFC Manning was operating in a broken system that limited public access to information would serve to explain the circumstances surrounding the alleged misconduct. Acknowledgment by Congress that at least some of the charged documents in this case were not properly classified may tend to lower PFC Manning’s punishment. As such, H.R. 553 is relevant and should be judicially noticed.

14. Mr. Thomas Blanton’s testimony before the House Judiciary Committee is proper for judicial notice because it is a relevant statement for which there is a hearsay exception. This Court has acknowledged that a “Congressional record could be admissible under MRE 803(8)(A) if relevant.” See Appellate Exhibit 356 at 12. Transcripts of Congressional hearings document the activities of Congress and are, thus, contemplated by M.R.E. 803(8)(A). Because Mr. Blanton testified before Congress and are included in the transcript of the Congressional hearing, his statements are properly admitted under M.R.E. 803(8)(A).

15. Hearsay concerns alleviated, Mr. Blanton's testimony is relevant at both the merits and any pre-sentencing phase. Mr. Blanton testified in part:

Mr. Chairman, it is a great honor for me, and Judge Gohmert and also to be in the middle of this extraordinary high-level tutorial in the Espionage Act and the Constitution. I feel like a grad student again; and it is a joy, actually. I also wanted to thank you, Mr. Chairman, for resurrecting my graveyard quote, that we have low fences around vast prairies of government secrets where we really need tall fences around small graveyards of the real secrets; and that is a core point I want to come back to today. I really have three points. One of them is the government always overreacts to leaks, always; and all you have to do is say the phrase "Watergate plumbers" and you know what I am talking about.

Back then, they were discussing firebombing the Brookings Institution on the chance there might still be a copy of the Pentagon papers in there. Today, you are having debates on FOX news: Let's do some targeted assassination attempts on Julian Assange. Well, I have to say G. Gordon Liddy would be right at home, and both is absurd. And the overreaction the government typically does is not to kill anybody or to firebomb something but to go right to the second major point I want to make today. They are going to classify more information.

What I am worried about most is the backlash. I mean, in my prepared statement, I have got multiple examples of all the estimates, and they range from 50 percent to 90 percent, of what the problem of overclassification really amounts to. Governor Tom Kean, head of the 9/11 Commission, after looking at all of the al Qaeda intelligence that we gathered before 9/11, said, you know, 75 percent of what I saw that was classified should not have been. And the Commission said we not only needed to do information sharing between the agencies, we had to do information sharing with the American people, because that is the only way we can really protect ourselves. What a great lesson that is.

The system is so overwhelmed with the secrets that we can no longer really protect the real ones and we can't let out the ones that would actually keep us all safer.

And I think it is a mistake to try to see this as a balancing test. It is not a balance between openness and security. The findings of the 9/11 Commission were that more openness would have made us more secure. That is what you do in an open society to keep yourself safe. You are not safer in the dark. You don't hide your vulnerabilities. You expose them and you fix them. That is how we proceed in America.

The third point I just want to make about where we are today. We are in the middle of a syndrome that one senior government official I really respect holds all the clearances, does the audits, pushes back against excessive secrecy, called it Wikimania. We are in the middle of Wikimania, and it is going to lead to so much

more heat than light. Targeted assassination is only the most extreme case, but look at all the other proposals we have got on the table and the front burners to try to push back, to punish WikiLeaks, to push back against speech. *See* Attachment C

He went on to testify:

I have to tell you, I wish every terrorist group in the world would write the U.S. ambassador in their local town, you know, days or a week before they are about to launch something, and ask the ambassador, hey, would you help us, you know, make sure nobody innocent gets hurt? Would you really work with us? We would be glad to talk to you.

And I understand why the ambassadors didn't believe them. Because WikiLeaks said, oh, and, by the way, we will keep anything you say to us confidential. It is hard to square with the previous statements of WikiLeaks.

But I wish every terrorist group would get into partnership with Le Monde and El Pais and the Guardian and the New York Times to assess what the damage might be, to redact their own documents, to put regulators on the bombs they drop. That would be a good thing. WikiLeaks is not terrorists. *Id.*

Like H.R. 553, evidence of overclassification makes it less likely that a document's classification marking put PFC Manning on notice that its disclosure could result in injury to the United State or benefit a foreign nation. M.R.E. 401. As such, Mr. Blanton's testimony is relevant on the merits. Likewise, it is relevant during any pre-sentencing phase because it establishes the circumstances surrounding PFC Manning's alleged misconduct. Evidence of consistent historical over-reaction to alleged unauthorized disclosures by the Government suggest yet another overreaction by the Government in PFC Manning's case. Such evidence would tend to mitigate PFC Manning's alleged misconduct and is, thus, relevant. R.C.M. 1001(c).

16. The proffered House of Representatives hearings from 2007 are also admissible and relevant. This Court has acknowledged that a "Congressional record could be admissible under MRE 803(8)(A) if relevant." *See* Appellate Exhibit 356 at 12. Transcripts of Congressional hearings document the activities of Congress and are, thus, contemplated by M.R.E. 803(8)(A). Because the proffered transcript documents the activities of Congress it falls under the hearsay exception offered by M.R.E. 803(8)(A).

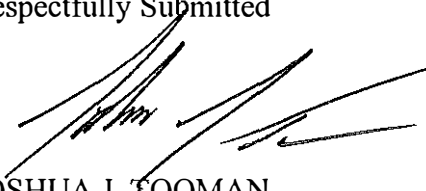
17. The proffered transcript is relevant on both the merits and during any necessary pre-sentencing phase. The transcript laid the foundation for the sentiment that Mr. Blanton and H.R. 553 would later echo: a shocking percentage of documents are wrongly classified. Included in the transcript is testimony from J. William Leonard, Director of Information Security Oversight Office at the National Archives and Records Administration. Mr. Leonard testified that a review by his office discovered that classification was clearly done correctly only 64% of the time. *See* Attachment D at 6. Thus, classification is wrong more than 1/3 of the time. Again, such evidence rebuts any argument that PFC Manning knew or should have known that a document

could cause injury to the United States or benefit a foreign nation based solely on the document's classification. Because the transcript makes an element of several charged Specifications less likely, it is relevant. M.R.E. 401. Likewise, the transcript is filled with evidence that establishes the circumstances under which PFC Manning was operating at the time of the alleged misconduct. Evidence that the classification system was broken and its condition had negative consequences for the nation would tend to shift some of the culpability from PFC Manning on to the system itself. Because such evidence could tend to lower PFC Manning's punishment it is relevant during any necessary pre-sentencing phase.

CONCLUSION

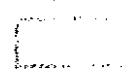
18. Based on the above, the Defense requests that the Court to take judicial notice of the requested adjudicate facts and law.

Respectfully Submitted



JOSHUA J. TOOMAN
CPT, JA
Defense Counsel

ATTACHMENT A

[Log In](#)[HOME](#) [BROWSE](#) [TRACK](#) [ABOUT](#) [US](#)[CONGRESS](#) [BILLS](#) [H.R. 553 \(111TH\)](#)

H.R. 553 (111th): Reducing Over-Classification Act

111th Congress, 2009–2010

To require the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information, and for other purposes.

Introduced: Jan 15, 2009

Sponsor: Rep. Jane Harman [D CA36]

Status: Signed by the President

Bill titles and the summary above are written by the sponsor.

H.R. stands for House of Representatives bill.

BILL OVERVIEW

STATUS:

| | |
|----------------------------|--------------|
| Introduced | Jan 15, 2009 |
| Passed House | Feb 03, 2009 |
| Passed Senate with Changes | Sep 27, 2010 |
| Passed Senate | Sep 28, 2010 |

RELATED BILLS:

[Search for similar bills.](#)

SUBJECT AREAS:

[Use these subject areas to explore related legislative activity.](#)

[Government Operations and Politics](#)

Signed by the President Oct 07,
2010

This bill was enacted after being
signed by the President on October
7, 2010.

TEXT: Read Bill Text

COSPONSORS: none

COMMITTEES: House Committee on Homeland
Security

Senate Committee on Homeland
Security and Governmental
Affairs

The committee chair determines
whether a bill will move past the
committee stage.

PRIMARY THOMAS (The Library of
SOURCE Congress)
THOMAS is updated generally
one day after events occur and
events since the last update may
not be reflected here.

CITATION This page can be cited in one of
these formats (click for details):
APA, MLA, Wikipedia Template.

(About Ads | Advertise H

Administrative law and
regulatory procedures
Administrative remedie
Congressional oversight
Department of Homelar
Security
Employment and trainin
programs
Government employee
benefits, personnel man
Government ethics and
transparency, public co
Government informatio
archives
Government investigati
Homeland security
Intelligence activities,
surveillance, classified
information
National Archives and F
Administration
Terrorism

OFFICIAL SUMMARY

This summary was written by the Congressional Service, a nonpartisan arm of the Library of Congress. GovTrack did not write and has no control over summaries.

10/7/2010--Public Law. (This measure has not amended since it was passed by the Senate on 27, 2010. The summary of that version is repeated.)
Reducing Over-Classification Act -

Section 4 -

Amends the Homeland Security Act of 2002 (HSA) to require the Secretary of Homeland Security (DHS) to c

Classified Information Advisory Officer to develop and disseminate educational materials and to develop and administer training programs to assist state, local, and tribal governments (including law enforcement agencies and private sector entities):

- (1) in developing plans and policies to respond to requests related to classified information without compromising information to individuals who lack appropriate security clearances;
- (2) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and
- (3) on the means by which such personnel may apply for security clearances.

Directs such Officer to inform the Under Secretary for Intelligence and Analysis on policies and procedures to facilitate the sharing of classified information with such personnel.

Section 5 -

Amends the National Security Act of 1947 to require the Director of National Intelligence to establish:

- (1) guidance to standardize formats for classified and unclassified intelligence products for purposes of preparing and sharing of such products; and
- (2) policies and procedures requiring the increased use, including portion markings, of the classification markings on information within one intelligence product.

Amends HSA to:

- (1) include among the responsibilities of the Secretary relating to intelligence and analysis and infrastructure to integrate relevant information, analysis, and vulnerability assessments in order to prepare finished intelligence information products in both classified and unclassified formats whenever reasonably expected to be of interest to state, local, or tribal government or a private sector entity; and
- (2) require the state, local, and tribal homeland security and law enforcement officers and intelligence analysts assigned by the Interagency Threat Assessment and Coordination Group (ITACG) Detail to work in the field.

Counterterrorism Center to make recommendations to the Secretary for the further dissemination of Intel products that could likely inform or improve the security of such a government or entity.

Requires the Secretary, in coordination with the Director of the National Counterterrorism Center and the Advisory Council, to:

(1) compile an annual assessment of ITACG Detail's performance, including summaries of customer fee-preparing, disseminating, and requesting the dissemination of intelligence products intended for state, local government and private sector entities;

(2) provide such assessment to the program manager for the information sharing environment for use in report on ITACG progress.

Requires such report to include an assessment of whether the ITACG detailees have appropriate access information as required.

Section 6 -

Permits the President or the head of an agency with an officer or employee who is authorized to make original or derivative classification decisions, in making certain cash incentive awards, to consider such officer's or employee's consistent and proper classification of information.

Requires the inspector general of each such agency, in consultation with the Information Security Oversight Board, to carry out at least two evaluations of that agency or components thereof to:

(1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted and effectively administered; and

(2) identify policies, procedures, rules, regulations, or management practices that may be contributing to misclassification of material.

Requires each first evaluation to be completed by September 30, 2013, and each second evaluation to be completed by September 30, 2016.

Requires each inspector general to:

(1) submit a report on each such evaluation to specified congressional committees, the agency head, and the Information Security Oversight Office; and

(2) coordinate with other inspectors general and with the Information Security Oversight Office to ensure evaluations follow a consistent methodology that allows for cross-agency comparisons.

Section 7 -

Directs the head of each executive agency, in accordance with Executive Order 13526, to require:

(1) annual training for each employee who has original classification authority; and

(2) training at least every two years for employees who perform derivative classification or are responsible for dissemination, preparation, production, receipt, publication, or otherwise communication of classified information.

Requires such training to:

(1) educate the employee regarding the guidance established under the National Security Act of 1947 re formatting of finished intelligence products, the proper use of classification markings, and incentives and related to the proper classification of intelligence information; and

(2) serve as a prerequisite for obtaining and maintaining original classification authority or derivatively classified information.

Directs each agency head to ensure that the training is conducted efficiently and in conjunction with any security, intelligence, or other training programs to reduce the associated costs and administrative burden.

[HOME](#)[BROWSE](#)[ABOUT](#)[GOVTRACK](#)[GOVTRACK BLOG](#)[FOR](#)[DEVELOPERS](#)[OTHER TOOLS](#)[LOG IN](#)

site INFORMATION

GovTrack.us is a project of Civic Impulse, LLC. Read about GovTrack.

Feedback is welcome to operations@govtrack.us, but we can't pass on messages to Members of Congress.

You are encouraged to reuse any material on this site. GovTrack supports other Congress-tracking websites through our open data.

[follow](#)[GOVTRACK](#)[FACEBOOK](#)[TWITTER](#)[GOVTRACK BLOG](#)

ATTACHMENT B

H.R. 553

One Hundred Eleventh Congress
of the
United States of America

AT THE SECOND SESSION

*Began and held at the City of Washington on Tuesday,
the fifth day of January, two thousand and ten*

An Act

To require the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information, and for other purposes.

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE.

This Act may be cited as the "Reducing Over-Classification Act".

SEC. 2. FINDINGS.

Congress finds the following:

(1) The National Commission on Terrorist Attacks Upon the United States (commonly known as the "9/11 Commission") concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies.

(2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.

(3) Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector.

(4) Over classification of information is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 486).

(5) Federal departments or agencies authorized to make original classification decisions or that perform derivative classification of information are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of classification markings and the policies of the National Archives and Records Administration.

SEC. 3. DEFINITIONS.

In this Act:

(1) DERIVATIVE CLASSIFICATION AND ORIGINAL CLASSIFICATION.—The terms "derivative classification" and "original classification" have the meanings given those terms in Executive Order No. 13526.

(2) EXECUTIVE AGENCY.—The term "Executive agency" has the meaning given that term in section 105 of title 5, United States Code.

(3) EXECUTIVE ORDER NO. 13526.—The term "Executive Order No. 13526" means Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) or any subsequent corresponding executive order.

SEC. 4. CLASSIFIED INFORMATION ADVISORY OFFICER.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

"SEC. 210F. CLASSIFIED INFORMATION ADVISORY OFFICER.

"(a) REQUIREMENT TO ESTABLISH.—The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

"(b) RESPONSIBILITIES.—The responsibilities of the Classified Information Advisory Officer shall be as follows:

"(1) To develop and disseminate educational materials and to develop and administer training programs to assist State, local, and tribal governments (including State, local, and tribal law enforcement agencies) and private sector entities—

"(A) in developing plans and policies to respond to requests related to classified information without communicating such information to individuals who lack appropriate security clearances;

"(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

"(C) on the means by which such personnel may apply for security clearances.

"(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with such personnel, as appropriate.

"(c) INITIAL DESIGNATION.—Not later than 90 days after the date of the enactment of the Reducing Over-Classification Act, the Secretary shall

"(1) designate the initial Classified Information Advisory Officer; and

"(2) submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a written notification of the designation."

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by inserting after the item relating to section 210E the following:

"Sec. 210F. Classified Information Advisory Officer."

SEC. 5. INTELLIGENCE INFORMATION SHARING.

(a) DEVELOPMENT OF GUIDANCE FOR INTELLIGENCE PRODUCTS.—Paragraph (1) of section 102A(g) of the National Security Act of 1947 (50 U.S.C. 403-1(g)) is amended—

- (1) in subparagraph (E), by striking “and” at the end;
- (2) in subparagraph (F), by striking the period at the end and inserting a semicolon and “and”; and

(3) by adding at the end the following:

“(G) in accordance with Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) (or any subsequent corresponding executive order), and part 2001 of title 32, Code of Federal Regulations (or any subsequent corresponding regulation), establish—

“(i) guidance to standardize, in appropriate cases, the formats for classified and unclassified intelligence products created by elements of the intelligence community for purposes of promoting the sharing of intelligence products; and

“(ii) policies and procedures requiring the increased use, in appropriate cases, and including portion markings, of the classification of portions of information within one intelligence product.”.

(b) CREATION OF UNCLASSIFIED INTELLIGENCE PRODUCTS AS APPROPRIATE FOR STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR STAKEHOLDERS.—

(1) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS AND INFRASTRUCTURE PROTECTION.—Paragraph (3) of section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is amended to read as follows:

“(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

“(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal Government, State, and local government, agencies and authorities, the private sector, and other entities; and

“(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.”.

(2) ITACG DETAIL.—Section 210D(d) of the Homeland Security Act of 2002 (6 U.S.C. 124k(d)) is amended—

(A) in paragraph (5)—

(i) in subparagraph (D), by striking “and” at the end;

(ii) by redesignating subparagraph (E) as subparagraph (F); and

(iii) by inserting after subparagraph (D) the following:

“(E) make recommendations, as appropriate, to the Secretary or the Secretary’s designee, for the further dissemination of intelligence products that could likely

inform or improve the security of a State, local, or tribal government, (including a State, local, or tribal law enforcement agency) or a private sector entity; and";

(B) in paragraph (6)(C), by striking "and" at the end;

(C) in paragraph (7), by striking the period at the end and inserting a semicolon and "and"; and

(D) by adding at the end the following:

"(8) compile an annual assessment of the ITACG Detail's performance, including summaries of customer feedback, in preparing, disseminating, and requesting the dissemination of intelligence products intended for State, local and tribal government (including State, local, and tribal law enforcement agencies) and private sector entities; and

"(9) provide the assessment developed pursuant to paragraph (8) to the program manager for use in the annual reports required by subsection (c)(2)."

(c) INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP ANNUAL REPORT MODIFICATION.—Subsection (c) of section 210D of the Homeland Security Act of 2002 (6 U.S.C. 124k) is amended—

(1) in the matter preceding paragraph (1), by striking ", in consultation with the Information Sharing Council,";

(2) in paragraph (1), by striking "and" at the end;

(3) in paragraph (2), by striking the period at the end and inserting a semicolon and "and"; and

(4) by adding at the end the following:

"(3) in each report required by paragraph (2) submitted after the date of the enactment of the Reducing Over-Classification Act, include an assessment of whether the details under subsection (d)(6) have appropriate access to all relevant information, as required by subsection (g)(2)(C)."

SEC. 6. PROMOTION OF ACCURATE CLASSIFICATION OF INFORMATION.

(a) INCENTIVES FOR ACCURATE CLASSIFICATIONS. In making cash awards under chapter 45 of title 5, United States Code, the President or the head of an Executive agency with an officer or employee who is authorized to make original classification decisions or derivative classification decisions may consider such officer's or employee's consistent and proper classification of information.

(b) INSPECTOR GENERAL EVALUATIONS.

(1) REQUIREMENT FOR EVALUATIONS.—Not later than September 30, 2016, the inspector general of each department or agency of the United States with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office, shall carry out no less than two evaluations of that department or agency or a component of the department or agency—

(A) to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and

(B) to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency or component.

(2) DEADLINES FOR EVALUATIONS.—

(A) INITIAL EVALUATIONS. Each first evaluation required by paragraph (1) shall be completed no later than September 30, 2013.

(B) SECOND EVALUATIONS.—Each second evaluation required by paragraph (1) shall review progress made pursuant to the results of the first evaluation and shall be completed no later than September 30, 2016.

(3) REPORTS.—

(A) REQUIREMENT. Each inspector general who is required to carry out an evaluation under paragraph (1) shall submit to the appropriate entities a report on each such evaluation.

(B) CONTENT.—Each report submitted under subparagraph (A) shall include a description of

(i) the policies, procedures, rules, regulations, or management practices, if any, identified by the inspector general under paragraph (1)(B); and

(ii) the recommendations, if any, of the inspector general to address any such identified policies, procedures, rules, regulations, or management practices.

(C) COORDINATION. The inspectors general who are required to carry out evaluations under paragraph (1) shall coordinate with each other and with the Information Security Oversight Office to ensure that evaluations follow a consistent methodology, as appropriate, that allows for cross-agency comparisons.

(4) APPROPRIATE ENTITIES DEFINED.—In this subsection, the term "appropriate entities" means—

(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate;

(B) the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives;

(C) any other committee of Congress with jurisdiction over a department or agency referred to in paragraph (1);

(D) the head of a department or agency referred to in paragraph (1); and

(E) the Director of the Information Security Oversight Office.

SEC. 7. CLASSIFICATION TRAINING PROGRAM.

(a) IN GENERAL.—The head of each Executive agency, in accordance with Executive Order 13526, shall require annual training for each employee who has original classification authority. For employees who perform derivative classification or are responsible for analysis, dissemination, preparation, production, receipt, publication, or otherwise communication of classified information, training shall be provided at least every two years. Such training shall

(1) educate the employee, as appropriate, regarding—

(A) the guidance established under subparagraph (G) of section 102A(g)(1) of the National Security Act of 1947 (50 U.S.C. 403-1(g)(1)), as added by section 5(a)(3), regarding the formatting of finished intelligence products;

(B) the proper use of classification markings, including portion markings that indicate the classification of portions of information; and

(C) any incentives and penalties related to the proper classification of intelligence information; and

(2) ensure such training is a prerequisite, once completed successfully, as evidenced by an appropriate certificate or other record, for—

(A) obtaining original classification authority or derivatively classifying information; and

(B) maintaining such authority.

(b) RELATIONSHIP TO OTHER PROGRAMS.—The head of each Executive agency shall ensure that the training required by subsection (a) is conducted efficiently and in conjunction with any other required security, intelligence, or other training programs to reduce the costs and administrative burdens associated with carrying out the training required by subsection (a).

Speaker of the House of Representatives.

*Vice President of the United States and
President of the Senate.*

ATTACHMENT C

**ESPIONAGE ACT AND THE LEGAL AND
CONSTITUTIONAL ISSUES RAISED BY WIKILEAKS**

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED ELEVENTH CONGRESS
SECOND SESSION

DECEMBER 16, 2010

Serial No. 111-160

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2011

63-081 PDF

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 612-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, Jr., Michigan, *Chairman*

| | |
|---------------------------------------|--|
| HOWARD L. BERMAN, California | LAMAR SMITH, Texas |
| RICK BOUCHER, Virginia | F. JAMES SENSENBRENNER, JR., Wisconsin |
| JERROLD NADLER, New York | HOWARD COBLE, North Carolina |
| ROBERT C. "BOBBY" SCOTT, Virginia | ELTON GALLEGLY, California |
| MELVIN L. WATT, North Carolina | BOB GOODLATTE, Virginia |
| ZOE LOFGREN, California | DANIEL E. LUNGREN, California |
| SHEILA JACKSON LEE, Texas | DARRELL E. ISSA, California |
| MAXINE WATERS, California | J. RANDY FORBES, Virginia |
| WILLIAM D. DELAHUNT, Massachusetts | STEVE KING, Iowa |
| STEVE COHEN, Tennessee | TRENT FRANKS, Arizona |
| HENRY C. "HANK" JOHNSON, JR., Georgia | LOUIE GOHMERT, Texas |
| PEDRO PIERLUISI, Puerto Rico | JIM JORDAN, Ohio |
| MIKE QUIGLEY, Illinois | TED POE, Texas |
| JUDY CHU, California | JASON CHAFFETZ, Utah |
| TED DEUTCH, Florida | TOM ROONEY, Florida |
| LUIS V. GUTIERREZ, Illinois | GREGG HARPER, Mississippi |
| TAMMY BALDWIN, Wisconsin | |
| CHARLES A. GONZALEZ, Texas | |
| ANTHONY D. WEINER, New York | |
| ADAM B. SCHIFF, California | |
| LINDA T. SANCHEZ, California | |
| DANIEL MAFFEI, New York | |
| JARED POLIS, Colorado | |

PERRY APELBAUM, *Majority Staff Director and Chief Counsel*
SEAN McLAUGHLIN, *Minority Chief of Staff and General Counsel*

CONTENTS

DECEMBER 16, 2010

| | Page |
|---|------|
| OPENING STATEMENTS | |
| The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary | 1 |
| The Honorable Louie Gohmert, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary | 3 |
| The Honorable William D. Delahunt, a Representative in Congress from the State of Massachusetts, and Member, Committee on the Judiciary | 4 |
| The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Member, Committee on the Judiciary | 5 |
| The Honorable Charles A. Gonzalez, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary | 5 |
| The Honorable Ted Poe, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary | 5 |
| WITNESSES | |
| Mr. Geoffrey R. Stone, Professor and former Dean, University of Chicago Law School | |
| Oral Testimony | 6 |
| Prepared Statement | 9 |
| Mr. Abbe David Lowell, Partner, McDermott Will & Emery, LLP | |
| Oral Testimony | 22 |
| Prepared Statement | 25 |
| Mr. Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP | |
| Oral Testimony | 39 |
| Prepared Statement | 41 |
| Mr. Gabriel Schoenfeld, Ph.D., Senior Fellow, Hudson Institute | |
| Oral Testimony | 48 |
| Prepared Statement | 50 |
| Mr. Stephen I. Vladeck, Professor of Law, American University | |
| Oral Testimony | 66 |
| Prepared Statement | 69 |
| Mr. Thomas S. Blanton, Director, National Security Archive, George Washington University | |
| Oral Testimony | 74 |
| Prepared Statement | 77 |
| Mr. Ralph Nader, Legal Advocate and Author | |
| Oral Testimony | 87 |

search of the truth and informing us all." He is also the founding editorial board member of freedominfo.org, a network of international freedom of information advocates.

I read your prepared statement with great enthusiasm, and we are happy to have you here today.

TESTIMONY OF THOMAS S. BLANTON, DIRECTOR, NATIONAL SECURITY ARCHIVE, GEORGE WASHINGTON UNIVERSITY

Mr. BLANTON. Mr. Chairman, it is a great honor for me, and Judge Gohmert and also to be in the middle of this extraordinary high-level tutorial in the Espionage Act and the Constitution. I feel like a grad student again; and it is a joy, actually.

I also wanted to thank you, Mr. Chairman, for resurrecting my graveyard quote, that we have low fences around vast prairies of government secrets where we really need tall fences around small graveyards of the real secrets; and that is a core point I want to come back to today.

I really have three points. One of them is the government always overreacts to leaks, always; and all you have to do is say the phrase "Watergate plumbers" and you know what I am talking about.

Back then, they were discussing firebombing the Brookings Institution on the chance there might still be a copy of the Pentagon papers in there. Today, you are having debates on FOX news: Let's do some targeted assassination attempts on Julian Assange.

Well, I have to say G. Gordon Liddy would be right at home, and both is absurd. And the overreaction the government typically does is not to kill anybody or to firebomb something but to go right to the second major point I want to make today. They are going to classify more information.

What I am worried about most is the backlash. I mean, in my prepared statement, I have got multiple examples of all the estimates, and they range from 50 percent to 90 percent, of what the problem of overclassification really amounts to. Governor Tom Kean, head of the 9/11 Commission, after looking at all of the al Qaeda intelligence that we gathered before 9/11, said, you know, 75 percent of what I saw that was classified should not have been. And the Commission said we not only needed to do information sharing between the agencies, we had to do information sharing with the American people, because that is the only way we can really protect ourselves. What a great lesson that is.

The system is so overwhelmed with the secrets that we can no longer really protect the real ones and we can't let out the ones that would actually keep us all safer.

And I think it is a mistake to try to see this as a balancing test. It is not a balance between openness and security. The findings of the 9/11 Commission were that more openness would have made us more secure. That is what you do in an open society to keep yourself safe. You are not safer in the dark. You don't hide your vulnerabilities. You expose them and you fix them. That is how we proceed in America.

The third point I just want to make about where we are today. We are in the middle of a syndrome that one senior government official I really respect holds all the clearances, does the audits,

pushes back against excessive secrecy, called it Wikimania. We are in the middle of Wikimania, and it is going to lead to so much more heat than light. Targeted assassination is only the most extreme case, but look at all the other proposals we have got on the table and the front burners to try to push back, to punish WikiLeaks, to push back against speech.

I think the problem here is we have got to look at each one of those proposals and say, is that really going to address the problem? Is it going to reduce government secrecy or is it going to add to it? Is it going to make us more safe? Is it going to make us more free? And do that test.

The Wikimania is really coming from a series of what in my statement I call Wikimyths. There has not been a documents dump. Everybody uses that phrase. There hasn't been one. The less than 2,000 cables are on the public record today out of that big database, and the editors of Le Monde and the Guardian and New York Times say that WikiLeaks is consulting with them about what to publish, what to redact and doing the dialogue with government officials in a pretty extraordinary, responsible way.

It is a very different posture, I should say, than WikiLeaks had even 6 or 8 months ago. I think the criticism they have gotten from journalists like us and from the public about endangering people's lives in Afghanistan and elsewhere, believe it or not, I think they have actually heard it.

There is no epidemic of leaks. In fact, all four of the big WikiLeaks publicity spats have come from a single person as far as we know, Bradley Manning, a young private.

So how do you solve the Bradley Manning problem? Well, you could do a pretty simple thing. The Defense Department has already done it. And here is a rational security policy. Just like you got two people to launch nuclear missiles, you have got two people to handle a communications manual that has codes in it, have two people before you can download something from a secure network. Pretty simple. That would have stopped Bradley Manning. Mormons send out two people as missionaries because that is how you have accountability, right? You don't have solos. All right.

There is no diplomatic meltdown from the WikiLeaks. I mean, there is a lot of heated rhetoric. But Secretary of Defense Robert Gates who ought to know—he served every President in my lifetime, as far as I can tell—and, Mr. Chairman, you quoted his remarks. Yeah, it is awkward, yeah, it is embarrassing, but, no, it is not a meltdown. It will make the job harder for diplomats. Maybe somebody is going to have to be reassigned. But, you know, in the long run, it is probably in the American national security interest for more foreign governments to be more accountable to their own citizens for their diplomacy. It is probably in our national security interest for the King of Saudi Arabia to actually be on the public record a little more often and the China politburo members to get exposed every now and then. That might be a long-term goal of what American national security diplomacy ought to be about.

And, finally, there is not a set of Wiki terrorists. I have heard that phrase batted around. They are not terrorists.

I have to tell you, I wish every terrorist group in the world would write the U.S. ambassador in their local town, you know, days or

a week before they are about to launch something, and ask the ambassador, hey, would you help us, you know, make sure nobody innocent gets hurt? Would you really work with us? We would be glad to talk to you.

And I understand why the ambassadors didn't believe them. Because WikiLeaks said, oh, and, by the way, we will keep anything you say to us confidential. It is hard to square with the previous statements of WikiLeaks.

But I wish every terrorist group would get into partnership with Le Monde and El Pais and the Guardian and the New York Times to assess what the damage might be, to redact their own documents, to put regulators on the bombs they drop. That would be a good thing. WikiLeaks is not terrorists.

And so that brings me to my final real point and recommendation to this Committee and to the prosecutors across the river in Alexandria: Just restraint. I know you don't usually have witnesses come up here and say, hey, let's all go take a nap. But you know in sleep-deprived Washington we might could use a little more restraint.

I would say leave the Espionage Act back in mothballs where it is right now and should stay. And in fact what we know is from some freedom of information requests there are still some classified documents from 1917 that will give the Espionage Act very good company. Don't mess with it. Leave it alone.

Our fundamental test should come out of Justice Stewart's dicta in the Pentagon papers case and some wonderful articles that Jack Goldsmith has actually written in the last couple of years where he says, look, our problem is, you know, the fundamental cause of leaks is a sense of illegitimacy that is bred by excessive government secrecy.

How do you address that? You reduce the secrecy. How do you deal with the legitimacy problem? You make sure as few secrets as possible are actually held and you protect those very strongly.

So the test is, for all these proposals, legislative and otherwise, does it send a signal that will actually reduce government secrecy? Does it send a signal that we need maximum possible disclosure, in Stewart's phrase, to have a system that actually has credibility and can protect the real secrets and where we can protect ourselves?

I thank you, Mr. Chairman, for this opportunity to engage in this debate. I hope it will reduce the mania a little bit and cut through some of the myths. Thank you, sir.

[The prepared statement of Mr. Blanton follows:]

PREPARED STATEMENT OF THOMAS S. BLANTON

Statement of Thomas Blanton
Director, National Security Archive, George Washington University
www.nsarchive.org

To the Committee on the Judiciary
U.S. House of Representatives

Hearing on the Espionage Act and the Legal and Constitutional
Implications of Wikileaks

Thursday, December 16, 2010
Rayburn House Office Building, Room 2141
Washington D.C.

Mr. Chairman, Ranking Member Smith, and members of the Committee, thank you for your invitation to testify today on the implications of the Wikileaks controversy. I am reminded of the ancient Chinese curse, "May you live in interesting times."

I have three main points to make today:

First, the government always overreacts to leaks, and history shows we end up with more damage from the overreaction than from the original leak.

Second, the government's national security classification system is broken, overwhelmed with too much secrecy, which actually prevents the system from protecting the real secrets. The rest should all come out.

Third, we are well into a syndrome that one senior government official called "Wikimania," where Wikimyths are common and there is far more heat than light – heat that will actually produce more leaks, more crackdowns, less accountable government, and diminished security.

By way of background, I should say right up front that my organization, the National Security Archive, has not gotten any 1.6 gigabyte thumbdrives in the mail in response to our many Freedom of Information Act requests, nor have we found any Bradley Mannings among the many highly professional FOIA officers who handle our cases. It's a lot more work to pry loose

national security documents the way we do it, but then it's a lot of work worth doing to make the rule of law a reality and give real force to the Freedom of Information Act.

It takes us years of research and interviews and combing the archives and the memoirs and the press accounts, even reading the agency phone books, to design and file focused requests that don't waste the government's time or our time but hone in on key documents and key decision points, then to follow up with the agencies, negotiate the search process, appeal the denials, even go to court when the stonewalling gets out of hand. Changing the iron laws of bureaucracy is a tall order, but we have allies and like-minded openness advocates in more than 50 countries now, passing access laws and opening Politburo and military dictators' files, poring through Communist Party records and secret police archives and death squad diaries, rewriting history, recovering memory, and bringing human rights abusers to trial.

Our more than 40,000 Freedom of Information requests have opened up millions of pages that were previously classified; we've published more than a million pages of documents on the Web and other formats; our staff and fellows have authored more than 60 books, one of which won the Pulitzer. Our Freedom of Information lawsuits have saved tens of millions of White House e-mail spanning from Reagan to Obama, whose Blackberry messages are now saved for posterity.

The George Foster Peabody Award in 1998 recognized our documentary contributions to CNN's *Cold War* series both from the Freedom of Information Act and from the Soviet archives; the Emmy Award in 2005 recognized our "outstanding achievement in news and documentary research"; and the George Polk Award citation (April 2000) called us "a FOIL'ers best friend" and used a wonderful phrase to describe what we do: "piercing the self-serving veils of government secrecy, guiding journalists in search for the truth, and informing us all."

Most pertinent to our discussion here today is our experience with the massive overclassification of the U.S. government's national security information. Later in this testimony I include some of the expert assessments by current and former officials who have grappled with the secrecy system and who estimate that between 50% to 90% of what is classified is either overclassified or should not be classified at all. That reality should restrain us from encouraging government prosecutors to go

after anybody who has unauthorized possession of classified information: such encouragement is an invitation for prosecutorial abuse and overreach -- exactly as we have seen in the case of the lobbyists for the American Israel Public Affairs Committee.

The reality of massive overclassification also points us towards remedies for leaks that are the opposite of those on the front burners such as criminalizing leaks. The only remedies that will genuinely curb leaks are ones that force the government to disgorge most of the information it holds rather than hold more information more tightly.

But a rational response to excessive government secrecy will be even more difficult to achieve in the current atmosphere of Wikimania. The heated calls for targeted assassinations of leakers and publishers remind me of the Nixon White House discussions of firebombing the Brookings Institution on suspicion of housing a copy of the Pentagon Papers. It was the earlier leak of the secret bombing of Cambodia that started President Nixon down the path to the Watergate plumbers, who began with righteous indignation about leaks, then moved to black bag jobs and break-ins and dirty tricks, and brought down the presidency. All the while, as the Doonesbury cartoon pointed out, only the American people and Congress were in the dark. One famous strip showed a Cambodian couple standing amid bomb wreckage, and the interviewer asks, was this from the secret bombing? Oh, no, not a secret at all, "I said, look Martha, here come the bombs."

Few have gone as far as Nixon, but overreaction to leaks has been a constant in recent American history. Almost every president has tied his White House in knots over embarrassing internal leaks; for example, the moment of greatest conflict between President Reagan and his Secretary of State George Shultz was not over the Iran-contra affair, but over the idea of subjecting Shultz and other high officials to the polygraph as part of a leak-prevention campaign. President Ford went from supporting to vetoing the Freedom of Information Act amendments of 1974 because of his reaction to leaks (only to be overridden by Congress). President George W. Bush was so concerned about leaks, and about aggrandizing presidential power, that his and Vice President Cheney's top staff kept the Deputy Attorney General, number two at Justice, out of the loop on the warrantless wiretapping program, and didn't even share legal opinions about the program with the top lawyers of the National Security Agency that was implementing the intercepts.

But even with this background, I have been astonished at the developments of the last week, with the Air Force and the Library of Congress blocking the Wikileaks web site, and warning their staff not to even peek. I should have known the Air Force would come up with something like this. The Archive's own Freedom of Information Act lawsuit over the last 5 years had already established that the Air Force created probably the worst FOIA processing system in the entire federal government -- the federal judge in our case ruled the Air Force had "miserably failed" to meet the law's requirements. But now, apparently, the worst FOIA system has found a mate in the worst open-source information system? This policy is completely self-defeating and foolish. If Air Force personnel do not look at the leaked cables, then they are not doing their job as national security professionals.

Comes now the Library of Congress, built on Thomas Jefferson's books, also blocking access to the Wikileaks site. On the LC blog, a repeated question has been when exactly are you going to cut off the *New York Times* site too? One might also ask, when will you remove Bob Woodward's books from the shelves?

Official reactions like these show how we are suffering from "Wikimania." Almost all of the proposed cures for Bradley Manning's leak of the diplomatic cables are worse than the disease. The real danger of Wikimania is that we could revert to Cold War notions of secrecy, to the kind of stovepipes and compartments that left us blind before 9/11, to mounting prosecutions under the Espionage Act that just waste taxpayers' money and ultimately get dropped, and to censorship pressure on Internet providers that emulates the Chinese model of state control rather than the First Amendment. So perhaps a first order of business should be to dissect some of what I call the "Wikimyths."

1. A document dump.

So far there has been no dump of the diplomatic cables. As of yesterday, there were fewer than 2,000 cables posted on the Web in the Wikileaks and media sites combined, and another 100 or so uploaded each day, not the 251,000 that apparently exist in the overall database as downloaded by Bradley Manning. And even that set of a quarter-million cables represents only a fraction of the total flow of cable traffic to and from the State

Department, simply the ones that State staff considered "reporting and other informational messages deemed appropriate for release to the US government interagency community" (the Foreign Affairs Manual explanation of the SIPDIS tag). According to the editors of *Le Monde* and *The Guardian*, Wikileaks is following the lead of the media organizations on which documents to post, when to do so, and what to redact from the cables in terms of source identities that might put someone at risk. Such behavior is the opposite of a dump. At the same time, an "insurance" file presumably containing the entire database in encrypted form is in the hands of thousands, and Wikileaks founder Julian Assange has threatened to send out the decrypt key, if and when his back is against the wall. So a dump could yet happen of the cables, and the prior record is mixed. A dump did begin of the Iraq and Afghan war logs, but once reporters pointed out the danger to local cooperators from being named in the logs, Wikileaks halted the dump and withheld some 15,000 items out of 91,000 Afghan records.

2. An epidemic of leaks.

While the quantity of documents seems huge (hundreds of thousands including the Iraq and Afghan materials), from everything we know to date, all four tranches of Wikileaks publicity this year have come from a single leaker, the Army private Bradley Manning, who is now behind bars. First, in April, was the helicopter video of the 2007 shooting of the Reuters cameramen. Then came the Iraq and Afghan war logs (highly granular situation reports for the most part) in July and October. Now we see the diplomatic cables from the SIPRNet. Between 500,000 and 600,000 U.S. military and diplomatic personnel were cleared for SIPRNet access, so a security official looking for a glass half full would point out that a human-designed security system with half a million potential error points ended up only with one.

A better contrast would be to compare the proposals for dramatic expansion of the Espionage Act into arresting foreigners, to the simple operational security change that the Defense Department has already implemented. The latter would have prevented Manning from doing his solo downloads onto CD, and we should ask which approach would be more likely to deter future Mannings. State Department officials were gloating last week that no embassy personnel could pull a Manning because State's version of the SIPRNet wouldn't allow downloads onto walk-away media like thumb drives or CDs. Defense's rejoinder was that its wide range of forward

operating bases, equipment crashes from dust storms and incoming fire, and often tenuous Internet connections – certainly compared to the usually cushy conditions inside embassies – meant some download capacity was essential. Now, just as nuclear missile launch requires two operators' keys, and the handling of sensitive communications intelligence manuals requires "two person integrity," and the Mormons send their missionaries out in pairs, a SIPRNet download would take two to tango.

3. A diplomatic meltdown.

Headline writers loved this phrase, aided and abetted by official statements like Secretary of State Hillary Clinton's characterization of the cables' release as an "attack on America" "sabotaging peaceful relations between nations." In contrast, the Secretary of Defense Robert Gates played down the heat, in a much more realistic assessment that bears repeating. Gates told reporters two weeks ago, "I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer and so on. I think these descriptions are fairly significantly overwrought.... Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest." Most international affairs scholars are calling the cables fascinating and useful, but at least so far nothing in the diplomatic cables compares to the impact on public policy in 2004 from the leak of the Abu Ghraib photographs, or other recent leaks of the existence of the secret prisons, or the torture memos, or the fact of warrantless wiretapping, or even the Pentagon Papers' contribution to the end of the Vietnam war.

4. Alternatively, no news here.

Wikileaks critics who were not bemoaning a global diplomatic meltdown often went to the opposite extreme, that is to say there was nothing really new in the Bradley Manning cables. The past two weeks' worth of front-page headlines in the leading newspapers and broadcasts around the world should lay this myth to rest. Folks with more news judgment than we have in this room are continuing to assign stories from the cables, and foreign media in particular are getting an education perhaps more valuable for their understanding of their own countries than of the U.S. Likewise, the blogs are full of lists of stories showing all the things we didn't know before the cables emerged. The real problem with the modern news media is evident from the fact that there are many more reporters clustered around the British

jail holding Assange, than there are reporters in newsrooms actually reading the substance of the documents. Celebrity over substance every time.

5. Wikiterrorists.

I wish all terrorist groups would write the local U.S. ambassador a few days before they are launching anything -- the way Julian Assange wrote Ambassador Louis Susman in London on November 26 to ask for suggestions on how to make sure nobody gets hurt. I can certainly understand the State Department's hostile response and refusal to engage with Assange in the kind of dialogue U.S. government officials routinely have with mainstream media, and were already having with the *New York Times* over these particular cables. Given Wikileaks's prior stance, who in State could possibly have taken at face value the phrase in the November 26 letter which says "Wikileaks will respect the confidentiality of the advice provided by the United States Government" about risk to individuals.

But I wish all terrorist groups would partner up with *Le Monde* and *El Pais* and *Der Spiegel* and *The Guardian*, and *The New York Times*, and take the guidance of those professional journalists on what bombs go off and when and with what regulators. Even to make the comparison tells the story -- Wikileaks is not acting as an anarchist group, even remotely as terrorists, but as a part of the media, as publishers of information, and even more than that -- the evidence so far shows them trying to rise to the standards of professional journalism.

I was quoted in Sunday's *New York Times* as saying "I'm watching Wikileaks grow up" as they embrace the mainstream media which "they used to treat as a cuss word." So far, with only a few mistakes to date, the treatment of the cables by the media and by Wikileaks has been very responsible, incorporating governmental feedback on potential damage, redacting names of sources, and even withholding whole documents at the government's request. Of course, Assange and his colleagues could revert to more adolescent behavior, since there is the threat out there of the encrypted "insurance" file that would be dropped like a pinata if the organization reaches dire straits. But even then, even if all the cables went online, most of us would condemn the recklessness of such an action, but the fundamental media and publisher function Wikileaks is serving would not change.

6. When the government says it's classified, our job as citizens is to salute.

Actually our job as citizens is to ask questions. I have mentioned that experts believe 50% to 90% of our national security secrets could be public with little or no damage to real security. A few years back, when Rep. Christopher Shays (R-CT) asked Secretary of Defense Donald Rumsfeld's deputy for counterintelligence and security how much government information was overclassified, her answer was 50%. After the 9/11 Commission reviewed the government's most sensitive records about Osama bin Laden and Al-Qaeda, the co-chair of that commission, former Governor of New Jersey Tom Kean, commented that "three-quarters of what I read that was classified shouldn't have been" – a 75% judgment. President Reagan's National Security Council secretary Rodney McDaniel estimated in 1991 that only 10% of classification was for "legitimate protection of secrets" – so 90% unwarranted. Another data point comes from the Interagency Security Classification Appeals Panel, over the past 15 years, has overruled agency secrecy claims in whole or in part in some 65% of its cases.

When two of the CIA's top officers retired and went into business, the *Washington Post's* Dana Hedgpeth asked them what was most surprising about being in the private sector. Cofer Black and Robert Richer responded that "much of the information they once considered top secret is publicly available. The trick, Richer said, is knowing where to look. 'In a classified area, there's an assumption that if it is open, it can't be as good as if you stole it,' Richer said. 'I'm seeing that at least 80 percent of what we stole was open.'" ("Blackwater's Owner Has Spies for Hire," by Dana Hedgpeth, *Washington Post*, November 3, 2007). And this was before the Bradley Manning leaks.

In the National Security Archive's collections, we have dozens of examples of documents that are classified and unclassified at the same time, sometimes with different versions from different agencies or different reviewers, all because the secrecy is so subjective and overdone. My own favorite example is a piece of White House e-mail from the Reagan years when top officials were debating how best to help out Saddam Hussein against the Iranians. The first version that came back from our Freedom of Information lawsuit had large chunks of the middle section blacked out on national security grounds, classified at the secret level as doing serious

damage to our national security if released. But the second version, only a week or so later, had almost no black in the middle, but censored much of the top and the bottom sections as secret. Slide the two versions together and you could read practically the entire document. The punch line is: This was the same reviewer both times, just with almost completely contradictory notions of what needed to stay secret.

The *Associated Press* reported last week (December 9, 2010) that reporter Matt Apuzzo's review of the Bradley Manning cables "unmasked another closely guarded fact: Much of what the government says is classified isn't much of a secret at all. Sometimes, classified documents contained little more than summaries of press reports. Political banter was treated as confidential government intelligence. Information that's available to anyone with an Internet connection was ordered held under wraps for years." The first example AP cited was a cable from the U.S. Embassy in Ottawa briefing President Obama in early 2009 for an upcoming trip to Canada, a cable which "included this sensitive bit of information, marked confidential: 'No matter which political party forms the Canadian government during your Administration, Canada will remain one of our staunchest and most like-minded of allies, our largest trading and energy partner, and our most reliable neighbor and friend.' The document could not be made public until 2019, for national security reasons," the AP reported.

Among other issues raised by the AP reporting is the fact that more than half of the Bradley Manning cables are themselves unclassified to begin with. Why did these items need to be buried inside a system that went up to the secret level? Why couldn't those unclassified cables go up on the State Department's own public Web site? Are they really all press summaries and administria? Do they need any further review such as for privacy or law enforcement issues? What objection would the government have to pre-empting Wikileaks by posting these – that somehow it would be rewarding illicit behavior?

Bringing the reality of overclassification to the subject of leaks, Harvard law professor Jack Goldsmith, who served President George W. Bush as head of the controversial Office of Legal Counsel at the Justice Department, has written, "A root cause of the perception of illegitimacy inside the government that led to leaking (and then to occasional irresponsible reporting) is, ironically, excessive government secrecy." Goldsmith went on, in what was otherwise a highly critical review of the *New York Times'*

coverage of wiretapping during the George W. Bush years ("Secrecy and Safety," by Jack Goldsmith, *The New Republic*, August 13, 2008), to point out, "The secrecy of the Bush administration was genuinely excessive, and so it was self-defeating. One lesson of the last seven years is that the way for the government to keep important secrets is not to draw the normal circle of secrecy tighter. Instead the government should be as open as possible...."

Goldsmith's analysis draws on the famous dicta of Justice Potter Stewart in the Pentagon Papers case: "When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion." In fact, Stewart observed, "the hallmark of a truly effective internal security system would be the maximum possible disclosure" since "secrecy can best be preserved only when credibility is truly maintained."

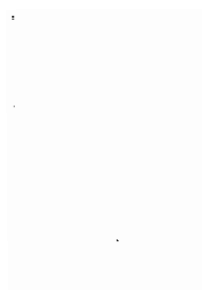
Between Goldsmith and Stewart, then, Mr. Chairman, we have a pretty good guide with which to assess any of the proposals that may come before you in the guise of dealing with Wikileaks in these next months. We have to ask, will the proposal draw the circle of secrecy tighter, or move us towards maximum possible disclosure? We have to recognize that right now, we have low fences around vast prairies of government secrets, when what we need are high fences around small graveyards of the real secrets. We need to clear out our backlog of historic secrets that should long since have appeared on the public shelves, and slow the creation of new secrets. And those voices who argue for a crackdown on leakers and publishers need to face the reality that their approach is fundamentally self-defeating because it will increase government secrecy, reduce our security, and actually encourage more leaks from the continued legitimacy crisis of the classification system.

Thank you for your consideration of these views, and I look forward to your questions.



ATTACHMENT D

(Please see separate e-mail attachment)



THE OVER-CLASSIFICATION AND
PSEUDO-CLASSIFICATION:
PART I, II, AND III

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE,
INFORMATION SHARING, AND
TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 22, 2007, APRIL 26, 2007, AND JUNE 28, 2007

Serial No. 110-20

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpoaccess.gov/congress/index.html>

U.S. GOVERNMENT PRINTING OFFICE

35-279 PDF

WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

| | |
|---|--------------------------------|
| LORETTA SANCHEZ, California, | PETER T. KING, New York |
| EDWARD J. MARKEY, Massachusetts | LAMAR SMITH, Texas |
| NORMAN D. DICKS, Washington | CHRISTOPHER SHAYS, Connecticut |
| JANE HARMAN, California | MARK E. SOUDER, Indiana |
| PETER A. DeFAZIO, Oregon | TOM DAVIS, Virginia |
| NITA M. LOWEY, New York | DANIEL E. LUNGREN, California |
| ELEANOR HOLMES NORTON, District of Columbia | MIKE ROGERS, Alabama |
| ZOE LOFGREN, California | BOBBY JINDAL, Louisiana |
| SHEILA JACKSON LEE, Texas | DAVID G. REICHERT, Washington |
| DONNA M. CHRISTENSEN, U.S. Virgin Islands | MICHAEL T. McCAUL, Texas |
| BOB ETHERIDGE, North Carolina | CHARLES W. DENT, Pennsylvania |
| JAMES R. LANGEVIN, Rhode Island | GINNY BROWN-WAITE, Florida |
| HENRY CUELLAR, Texas | MARSHA BLACKBURN, Tennessee |
| CHRISTOPHER P. CARNEY, Pennsylvania | GUS M. BILIRAKIS, Florida |
| YVETTE D. CLARKE, New York | DAVID DAVIS, Tennessee |
| AL GREEN, Texas | |
| ED PERLMUTTER, Colorado | |
| VACANCY | |

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*

TODD GEE, *Chief Counsel*

ROSALINE COHEN, *Chief Counsel*,

MICHAEL TWINCHEK, *Chief Clerk*

ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND
TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

| | |
|---|---|
| NORMAN D. DICKS, Washington | DAVID G. REICHERT, Washington |
| JAMES R. LANGEVIN, Rhode Island | CHRISTOPHER SHAYS, Connecticut |
| CHRISTOPHER P. CARNEY, Pennsylvania | CHARLES W. DENT, Pennsylvania |
| ED PERLMUTTER, Colorado | PETER T. KING, New York (<i>Ex Officio</i>) |
| BENNIE G. THOMPSON, Mississippi (<i>Ex Officio</i>) | |

THOMAS M. FINAN, *Director and Counsel*

BRANDON DECLER, *Counsel*

NATALIE NIXON, *Deputy Chief Clerk*

DERON McELROY, *Minority Senior Professional Staff Member*

(II)

CONTENTS

| | Page |
|--|------|
| STATEMENTS | |
| The Honorable Jane Harman, a Representative in Congress from the State of California, and Chairman, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment | 1 |
| The Honorable David G. Reichert, a Representative in Congress from the State of Washington, and Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment | 3 |
| The Honorable Bennie G. Thompson, a Representative in Congress from the State of Mississippi, and Chairman, Committee on Homeland Security .. | 4 |
| The Honorable Charles W. Dent, a Representative in Congress from the State of Pennsylvania | 22 |
| The Honorable Christopher P. Carney, a Representative in Congress from the State of Pennsylvania | 84 |
| The Honorable James R. Langevin, a Representative in Congress from the State of Rhode Island | 21 |
| WITNESSES | |
| THURSDAY, MARCH 22, 2007, PART I | |
| PANEL I | |
| Mr. Scott Armstrong, Founder, Information Trust | 9 |
| Ms. Meredith Fuchs, General Counsel, The National Security Archive, George Washington University: | |
| Oral Statement | 11 |
| Prepared Statement | 14 |
| Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration: | |
| Oral Statement | 5 |
| Prepared Statement | 7 |
| PANEL II | |
| Mr. Michael P. Downing, Assistant Commanding Officer, Counter-Terrorism/ Criminal Intelligence Bureau, Los Angeles Police Department: | |
| Oral Statement | 29 |
| Prepared Statement | 31 |
| Chief Cathy L. Lanier, Metropolitan Police Department, Washington, DC: | |
| Oral Statement | 24 |
| Prepared Statement | 26 |
| THURSDAY, APRIL 26, 2007, PART II | |
| PANEL I | |
| Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence: | |
| Oral Statement | 46 |
| Prepared Statement | 48 |

(III)

IV

| | Page |
|---|------|
| Dr. Carter Morris, Director, Informational Sharing and Knowledge Management, Office of Intelligence and Analysis, U.S. Department of Homeland Security: | |
| Oral Statement | 52 |
| Prepared Statement | 54 |
| Mr. Wayne M. Murphy, Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation: | |
| Oral Statement | 57 |
| Prepared Statement | 59 |

PANEL II

| | |
|--|----|
| Mr. Mark Zadra, Assistant Commissioner, Florida Department of Law Enforcement: | |
| Oral Statement | 66 |
| Prepared Statement | 68 |

THURSDAY, JUNE 28, 2007, PART III

| | |
|--|----|
| Mr. Mark Agrast, Senior Fellow, Center for American Progress: | |
| Oral Statement | 94 |
| Prepared Statement | 95 |
| Mr. Scott Armstrong, Founder, Information Trust: | |
| Oral Statement | 84 |
| Prepared Statement | 86 |
| Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Record Administration | 83 |
| Ms. Suzanne E. Spaulding, Principal, Bingham Consulting Group LLC: | |
| Oral Statement | 90 |
| Prepared Statement | 92 |

FOR THE RECORD

MARCH 22, 2009, PART I

| | |
|-------------------------------|-----|
| Prepared Statements: | |
| Hon. Jane Harman | 111 |
| Hon. Bennie G. Thompson | 113 |

APRIL 26, 2009, PART II

| | |
|--|----|
| Prepared Statement: | |
| Colonel Bart R. Johnson, New York State Police | 40 |

THE IMPACT ON INFORMATION SHARING PART I

Thursday, March 22, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 10:09 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chairwoman of the subcommittee] presiding.

Present: Representatives Harman, Langevin, Thompson, Reichert, and Dent.

Ms. HARMAN. [Presiding.] The subcommittee will come to order.

The chair apologizes for a late start. Even though my party is in the majority, I don't run the schedule here, and there was a conflicting hearing on emergency interoperability, and I was asking questions of witnesses. And that subject, obviously, is directly relevant to some of the tasks of this subcommittee, so I hope you will forgive me.

A recurrent theme throughout the 9/11 Commission's report was the need to prevent widespread over-classification by the federal government. The commission found that over-classification interferes with sharing critical information and impedes efficient responses to threats.

The numbers tell us we are still not heeding the commission's warning. Eight million new classification actions in 2001 jumped to 14 million new actions in 2005, while the quantity of declassified pages dropped from 100 million in 2001 to 29 million in 2005. In fact, some agencies were recently discovered to be withdrawing archived records from public access and reclassifying them.

Expense is also a problem. \$4.5 billion spent on classification in 2001 increased to \$7.1 billion in 2004, while declassification costs fell from \$232 million in 2001 to \$48.3 million in 2004.

In addition, an increasing number of policies to protect sensitive but unclassified from a range of federal agencies and departments has begun to have a dramatic impact. At the federal level, over 28 distinct policies for the protection of this information exists—28 distinct policies. That is almost as many policies as we have watch lists—that was intended to be humorous.

Unlike classified records, moreover, there is no monitoring of, or reporting on, the use or impact of protective, sensitive, unclassified information markings. The proliferation of these pseudo-classifica-

tions is interfering with the interagency information sharing, increasing the cost of information security and limiting public access.

Case in point, this document from the Department of Homeland Security. This document, which I cannot release to you or the press, is called, "Special Assessment: Radicalization in the State of California," a survey, and it is dated the 22nd of November, 2006.

In a few weeks, I will be leading a field hearing to Torrance, California to examine the issues of domestic radicalization and homegrown terrorism, but this DHS document, a survey, as I mentioned, is marked, "unclassified, for official use only."

On page one, in a footnote, the survey states that it cannot be released "to the public, the media or other personnel who do not have a valid need to know without prior approval of an authorized DHS official."

Our staff requested and was denied an approval. Staff also asked for a redacted version of the document so we could use at least some of its contents at the coming California hearing. DHS was unable to provide one.

Let me be clear, and I say this as someone who served for 8 years on the House Intelligence Committee, I am not denying that there may be sensitive information included in this survey and in lots of products prepared by our government, but it illustrates my point.

What good is unclassified information about threats to the homeland if we can't even discuss them at a public hearing where the public is supposed to understand what some of those threats may be? How can we expect DHS and others to engage the public on important issues like domestic radicalization if we hide the ball?

Unfortunately, this is nothing new. In 1997, the Moynihan Commission stated that the proliferation of these new designations are often mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information.

These continuing trends are an obstacle to information sharing across the federal government and vertically with state, local and tribal partners, including most especially with our partners in the law enforcement community.

And in our second panel, we are going to hear from some of those partners, including Chief Lanier, and I want to welcome her today and congratulate her again on being one of the youngest ever police chiefs in the nation and a very well-qualified person to hold this position.

Until we have a robust intelligence and information-sharing system in place in this country with a clear and understandable system of classification, we run the risk of not being able to prevent a terrorist attack on the scale of 9/11 or greater, and I would even add on the scale of 9/11 or smaller. We are hurting ourselves by the way we unnecessarily protect information.

This is why this subcommittee will focus some of its efforts in the 110th Congress on improving information sharing with our first preventers, the men and women of state, local and tribal law enforcement who are the eyes and ears on our frontlines. We will do this work in the right way, partnering with our friends in the pri-

vacy and civil liberties community who want to protect America while serving our cherished rights.

I would like to extend a warm welcome to our witnesses who will be talking about these issues, first, some organizations, and then, two, on the frontlines in our law enforcement organizations.

On our first panel, we have assembled an array of experts who will be testifying about the extent of these problems and where are things are trending, and, as I mentioned, our second panel will give us some real-life experiences where classification—and I don't want to put words in their mouths, but I have read their testimony—is an obstacle rather than some form of benefit to them in their role to prevent, disrupt and protect the American public.

In addition, I hope witnesses will provide some constructive suggestions about how we might solve this problem, with the goal of ensuring the flow of information, the unfettered flow of necessary information between the federal government and state, local and tribal governments.

Welcome to all.

I now yield to the ranking member for opening remarks.

Mr. REICHERT: Thank you, Madam Chair, and thank you for organizing this hearing. It is a pleasure to be here this morning.

And thank all of you for being here in time from your busy schedule to come and testify before us.

We are all here this morning to discuss one of the subcommittee's major priorities, this over-classification and pseudo-classification. Over-classification, as most of you know, refers to decisions by the federal government to routinely restrict access to information using the designation, "confidential," "secret" or "top-secret."

Pseudo-classification is a similar practice applied to sensitive but unclassified information. This practice involves federal, state or local entities adding restrictions based on internal policies. The GAO has found that there are at least 56 different sensitive but unclassified designations at the federal level—56.

Common examples include, "for official use only," "sensitive but unclassified," "sensitive security information," and "law enforcement sensitive." Some of these designations make sense; some don't. Some, there is a real need to protect classified and sensitive information from disclosure.

In a world where virtually piece of unclassified information is available on the Internet, we need to ensure that what needs to be protected remains protected. The lives of our federal, state and local agents in the field often depend on it.

But as a classic military strategist once said, "If you try to protect everything, you wind up protecting nothing." The more secrets you keep, the harder they are to keep. I can't tell you how many times I have emerged from a secret briefing only to find out that everything that I have just learned has already been in the newspaper.

As a former sheriff, I have vivid memories of the federal government telling me that I could not access information that I needed to do my job because it was classified or otherwise restricted. And I have also watched as the federal government has taken sensitive information from the state and local law enforcement and treated it without regard for its sensitivity.

I am just going to share a real brief story with you. Years ago, when we arrested our suspect in the Green River murder case, a serial murder case nationally known, internationally known as one of the worst serial murder cases in the world of 50 victims, the FBI was a part of that team. They produced paperwork connected and associated with that case.

Once the person was arrested and charged, of course, there was a request by the defense attorney for information. The FBI would not release the information to substantiate and help our case because they said it was classified.

The fear there was this: Of course, they had information that we would have lost our case. Eventually, they came forward, presented the information for discovery; however, the fear was that because of the state laws that existed in the state of Washington, everything they disclosed then would be subject to public disclosure laws. So anything they released to us, the sheriff's office is required by state law to give that to the news media. So that was their concern.

We have a lot of issues here to discuss today. I am not going to finish the rest of my statement. We are just happy to have you here, and you know that we understand the problem, and we are looking to help you find solutions.

Thank you.

Ms. HARMAN. I thank the ranking member and note that his experience as a sheriff is extremely useful to this subcommittee as we pursue issues like this.

The chair now recognizes the chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you, Madam Chair. I join you in welcoming our distinguished witnesses today to this important hearing on the problem of over-and pseudo-classification of intelligence.

Information sharing between the federal government and its state, local and tribal partners is critical to making America safer, but we won't get there if all we have is more and more classification and more and more security clearances for people who need access to that classified information.

The focus should be different. The federal government instead must do all it can to produce intelligence products that are unclassified. Unclassified intelligence information is what our nation's police officers, first responders and private sector partners need most. They have told me time and time again that what they don't need is information about intelligence sources and methods.

And I think all of us have been in enough briefings that were somehow classified at varying levels only to see it on the evening news and be shocked that, well, why would you keep it from members of Congress when all we have to do is delay the briefing 6 hours and we can see it? That occurred last week.

I am sure Mr. Langevin understands very well. We had a briefing that we were told that was top-secret, took the BlackBerrys, took the cell phones, and, lo and behold, it was on the 5 p.m. news.

So to some degree, the over-classification is a problem.

If we are going to successfully address terrorism, then we have to share the information in real time and trust our partners to

some degree. If we can't trust law enforcement, if we can't trust first responders, who can we trust?

So I think it is a hearing that is pertinent to the challenge that we face. I look forward to the testimony of the witnesses, and, obviously, this is one of many, Madam Chair. I am sure we will be participating in over this session.

I yield back.

Ms. HARMAN. I thank the chairman and would point out that other members of the subcommittee can submit opening statements for the record, under our rules.

I now welcome our first panel of witnesses.

Our first witness, Mr. Bill Leonard, is the director of the Information Security Oversight Office at the National Archives. Mr. Leonard's office has policy oversight of the entire federal government-wide security classification system—that is a mouthful—and he reports directly to the president.

His office receives his policy and program guidance from the national Security Council. More than 60 executive branch agencies create or handle classified national security information, and Mr. Leonard's work in this capacity impacts all of them.

Welcome, Mr. Leonard.

Our second witness is my Washington, D.C., neighbor and good friend, Scott Armstrong. Mr. Armstrong is the executive director of Information Trust, a nonprofit group that works toward opening access to government information.

He has been inducted into the FOIA Hall of Fame—congratulations—and was awarded the James Madison Award by the American Library Association in 1992. Mr. Armstrong has been a Washington Post reporter and is the founder of the National Security Archive at George Washington University.

Our third witness, Meredith Fuchs, serves as the general counsel to the nongovernmental National Security Archives. At the Archives, she oversees Freedom of Information Act, called FOIA, and anti-secrecy litigation and frequently lectures on access to government information.

She has supervised five government-wide audits of federal agency FOIA performance and one focused on the proliferation of sensitive but unclassified information labels.

Without objection, the witnesses' full statements will be inserted in the record, and I would hope you could summarize in 5 minutes or less—we have a little timer for your benefit—your written testimony, and then hopefully we can have a lively exchange of views.

Let's start with Mr. Leonard.

**STATEMENT OF J. WILLIAM LEONARD, DIRECTOR,
INFORMATION SECURITY OVERSIGHT OFFICE, NATIONAL
ARCHIVES AND RECORDS ADMINISTRATION**

Mr. LEONARD. Chairwoman Harman, Mr. Reichert, Chairman Thompson and members of the subcommittee, I wish to thank you for holding this hearing this morning on issues relating to the very real challenge of over-classification.

The classification system and its ability to restrict the dissemination of information, the unauthorized disclosure of which would result in harm to our nation and its citizens, represents a funda-

mental tool at the government's disposal to provide for the common defense.

As with any tool, the classification system is subject to misuse and misapplication. When information is improperly declassified or not classified in the first place, although clearly warranted, our citizens, our democratic institutions, our homeland security and our interactions with foreign nations can be subject to potential harm.

Conversely, too much classification or the failure to declassify information as soon as it no longer satisfies the standards for continued classification unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of government.

In the final analysis, inappropriate classification activity of any nature undermines the integrity of the entire process and diminishes the effectiveness of this critical national security tool.

In this time of constant and unique challenges to our national security, it is the duty of all of us engaged in public service to do everything possible to enhance the effectiveness of this tool. To be effective, the classification process is a tool that must be wielded with precision. Few, if any, both within and outside of government, would deny that too much of the information produced by our agencies is classified.

In an audit of agency classification activity conducted by my office approximately one year ago, we discovered that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it clearly right only 64 percent of the time in making determinations as to the appropriateness of classification. This is emblematic of the daily challenges confronting agencies when ensuring that the 3 million plus cleared individuals with at least a theoretical ability to derivatively classify information get it right each and every time.

In response to the findings of this audit, last year I wrote to all agency heads and made a number of recommendations for their consideration. Collectively, these recommendations help preserve the integrity of the classification system while at the same time reduce inefficiencies and cost. I have included a list of these recommendations in my prepared formal testimony.

Recognizing that a focus of this hearing includes policies and procedures for handling sensitive, unclassified information, it is important to articulate recent initiatives by the president to ensure the robust and effective sharing of terrorism information vital to protecting Americans and the homeland from terrorist attacks.

To that end, the president has mandated the standardization of procedures for designated marking and handling sensitive but unclassified information across the federal government. Once implemented, our nation's defenders will be able to share controlled, unclassified information more rapidly and confidently.

The existence of such an option should significantly reduce the incentive to over-classify information. That happens now, in part, due to the absence of a dependable regime for the proper protection of sensitive information which should not be classified.

Again, thank you for inviting me here this morning, Madame Chair, and I would be happy to answer your questions or those that the subcommittee might have.

[The statement of Mr. Leonard follows:]

PREPARED STATEMENT OF J. WILLIAM, LEONARD

MARCH 22, 2007

Chairwoman Harman, Mr. Reichert, and members of the subcommittee, I wish to thank you for holding this hearing on issues relating to the very real challenge of overclassification of information within the Federal Government as well as for inviting me to testify today.

By section 5.2 of Executive Order 12958, as amended, "Classified National Security Information" (the Order), the President established the organization I direct, the Information Security Oversight Office, often called "ISOO." We are within the National Archives and Records Administration and by law and Executive order (44 U.S.C. 2102 and sec. 5.2(b) of E.O. 12958) are directed by the Archivist of the United States, who appoints the Director of ISOO, subject to the approval of the President. We also receive policy guidance from the Assistant to the President for National Security Affairs. Under the Order and applicable Presidential guidance, ISOO has substantial responsibilities with respect to the classification, safeguarding, and declassification of information by agencies within the executive branch. Included is the responsibility to develop and promulgate directives implementing the Order. We have done this through ISOO Directive No. 1 (32 CFR Part 2001) (the Directive).

The classification system and its ability to restrict the dissemination of information the unauthorized disclosure of which would result in harm to our nation and its citizens represents a fundamental tool at the Government's disposal to provide for the "common defense." The ability to surprise and deceive the enemy can spell the difference between success and failure on the battlefield. Similarly, it is nearly impossible for our intelligence services to recruit human sources who often risk their lives aiding our country or to obtain assistance from other countries' intelligence services, unless such sources can be assured complete and total confidentiality. Likewise, certain intelligence methods can work only if the adversary is unaware of their existence. Finally, the successful discourse between nations often depends upon confidentiality and plausible deniability as the only way to balance competing and divergent national interests.

As with any tool, the classification system is subject to misuse and misapplication. When information is improperly declassified, or is not classified in the first place although clearly warranted, our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations can be subject to potential harm. Conversely, too much classification, the failure to declassify information as soon as it no longer satisfies the standards for continued classification, or inappropriate reclassification, unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of government. In the final analysis, inappropriate classification activity of any nature undermines the integrity of the entire process and diminishes the effectiveness of this critical national security tool. Consequently, inappropriate classification or declassification puts today's most sensitive secrets at needless increased risk.

The challenge of overclassification is not new. Over 50 years ago, Congress established the Commission on Government Security (known as the "Wright Commission"). Among its conclusions, which were put forth in 1955, at the height of the Cold War, was the observation that overclassification of information in and of itself represented a danger to national security. This observation was echoed in just about every serious review of the classification systems since to include: the Commission to review DoD Security Policies and Practices (known as the "Stillwell Commission") created in 1985 in the wake of the Walker espionage case; the Joint Security Commission established during the aftermath of the Ames espionage affair; and the Commission on Protecting and Reducing Government Secrecy (otherwise known as the "Moynihan Commission"), which was similarly established by Congress and which issued its report in 1997.

More recently, the National Commission on Terrorist Attacks on the United States (the "9 11 Commission"), and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the "WMD Commission") likewise identified overclassification of information as a serious challenge.

It is Executive Order 12958, as amended, that sets forth the basic framework and legal authority by which executive branch agencies may classify national security information. Pursuant to his constitutional authority, and through the Order, the President has authorized a limited number of officials to apply classification to certain national security related information. In delegating classification authority the

President has established clear parameters for its use and certain burdens that must be satisfied.

Specifically, every act of classifying information must be traceable back to its origin as an explicit decision by a responsible official who has been expressly delegated original classification authority. In addition, the original classification authority must be able to identify or describe the damage to national security that could reasonably be expected if the information was subject to unauthorized disclosure. Furthermore, the information must be owned by, produced by or for, or under the control of the U. S. Government; and finally, it must fall into one or more of the categories of information specifically provided for in the Order.¹

The President has also spelled out in the Order some very clear prohibitions and limitations with respect to the use of classification. Specifically, for example, in no case can information be classified in order to conceal violations of law, inefficiency, or administrative error, to restrain competition, to prevent embarrassment to a person, organization, or agency, or to prevent or delay the release of information that does not require protection in the interest of national security.

It is the responsibility of officials delegated original classification authority to establish at the time of their original decision the level of classification (Top Secret, Secret, and Confidential), as well as the duration of classification, which normally will not exceed ten years but in all cases cannot exceed 25 years unless an agency has received specific authorization to extend the period of classification.

As I stated earlier, the ability and authority to classify national security information is a critical tool at the disposal of the Government and its leaders to protect our nation and its citizens. In this time of constant and unique challenges to our national security, it is the duty of all of us engaged in public service to do everything possible to enhance the effectiveness of this tool. To be effective, the classification process is a tool that must be wielded with precision. Few, if any, both within and outside Government, would deny that too much of the information produced by our agencies is classified. In an audit of agency classification activity conducted by my office approximately one year ago, we discovered that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it clearly right only 64 percent of the time in making determinations as to the appropriateness of classification. This is emblematic of the daily challenges confronting agencies when ensuring that the 3 million plus cleared individuals with at least theoretical ability to derivatively classify information get it right each and every time.

In response to the findings of this audit, last year I wrote to all agency heads and made a number of recommendations for their consideration. Collectively, these recommendations help preserve the integrity of the classification system while at the same time reduce inefficiencies and cost. They included:

- Emphasizing to all authorized holders of classified information the affirmative responsibility they have under the Order to challenge the classification status of information that they believe is improperly classified (§ 1.8(a) of the Order).
- Requiring the review of agency procedures to ensure that they facilitate classification challenges (§ 1.8(b) of the Order). In this regard, agencies were encouraged to consider the appointment of impartial officials whose sole purpose is to seek out inappropriate instances of classification and to encourage others to adhere to their individual responsibility to challenge classification, as appropriate.
- Ensuring that quality classification guides of adequate specificity and clarity are prepared and updated to further accurate and consistent derivative classification decisions (§ 2.2 of the Order).
- Ensuring the routine sampling of recently classified information to determine the propriety of classification and the application of proper and full markings (§ 5.4(d)(4) of the Order). Consideration should be given to reporting the results of these reviews to agency personnel as well as to the officials designated above who would be responsible to track trends and assess the overall effectiveness of the agency's efforts and make adjustments, as appropriate.

¹ Pursuant to § 1.4 of the Order, information shall not be considered for classification unless it concerns: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) weapons of mass destruction.

- Ensuring that information is declassified as soon as it no longer meets the standards for classification (?3.1(a) of the Order).
- Ensuring that prior to exercising the national security exemption as set forth in 5 U.S.C. 552b(1) when responding to FOIA requests, that agency personnel verify that the information involved clearly meets the standards for continued classification irrespective of the markings, to include declassification instructions, contained on the document.

Recognizing that a focus of this hearing includes policies and procedures for handling sensitive unclassified information, it is important to articulate recent initiatives by the President to ensure the robust and effective sharing of terrorism information vital to protecting Americans and the Homeland from terrorist attacks. To that end, the President has promulgated a set of guidelines and requirements that represent a significant step in the establishment of the Information Sharing Environment (ISE) called for by section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

Specifically, to promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, the President has mandated the standardization of procedures for designating, marking, and handling SBU information across the Federal Government. A clear mandate for achieving this goal has been laid out for the entire Executive branch and significant progress is underway to develop for the President's consideration standardized procedures for handling controlled unclassified information. Once implemented, our nation's defenders will be able to share controlled unclassified information more rapidly and confidently. The existence of such an option should significantly reduce the incentive to overclassify information. This happens now, in part, due to the absence of a dependable regime for the proper protection of sensitive information which should not be classified.

Again, I thank you for inviting me here today, Madame Chairwoman, and I would be happy to answer any questions that you or the subcommittee might have at this time.

Ms. HARMAN. I thank the witness.
Now, we will hear from Mr. Armstrong.

STATEMENT OF SCOTT ARMSTRONG, FOUNDER, INFORMATION TRUST

Mr. ARMSTRONG. Thank you, Madam Chair. Thank you. I am pleased to be able to discuss these issues with this subcommittee, given the membership of the subcommittee and the full committee include many of the people that have provided the leadership, or attempted to provide the leadership, to dig into these difficult questions on this committee and other committees of the Congress.

I am here on my own, of course, but I also would like to note that I participate in a dialogue, which is presently sponsored by the Aspen Institute, between the senior journalists, editors, publishers and high-level U.S. government officials from various national security intelligence agencies.

The purpose of the dialogue has been to address recurring concerns about the handling of classified information, the fact that sensitive information can find its way into the major media and could potential cause damage.

The discussions have included the attorney general, the director of Central Intelligence, the deputy director of National Intelligence, ranking members from the National Security Council, the Department of Defense, the National Security Agency, the FBI, the CIA, the Department of Homeland Security and the Department of Justice.

The dialogue is continuing with a variety of initiatives that I hope will further involve members of this committee and your col-

leagues and members of your staff, and we will be in consultation with you on that issue.

I would like to note three major areas today out of my testimony. Twenty-two years ago, in 1985, when I left the Washington Post, to found the National Security Archive, I went to the man who was then considered the maven of secrecy in the Reagan administration, General Richard Stillwell, and I developed an interesting and productive dialogue with General Stillwell who was chairing a commission to examine systemic vulnerabilities in the classification system.

At that time, the Reagan administration's concern was not so much news media leaks but the fact that there were significant leaks in the form of espionage. General Stillwell not only quoted, and usually misquoted, a sentence in Supreme Court Justice Potter Stewart's concurrence in the Pentagon Papers case, "When everything is classified, then nothing is classified," but he finished that sentence, "And the system becomes one to be disregarded by the cynical or the careless and to be manipulated by those intent on self-protection or self-promotion."

Like Justice Stewart, General Stillwell believed that the hallmark of a truly effective internally security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is maintained.

Regrettably, the system then pertained a systemic use of special access programs and other compartmented intelligence controls by those that have now been extended even on classified information and created a labyrinth of security measures, often unaccountable and sometimes wholly unauthorized. That situation has not changed in the ensuing 20 years.

My experience has reinforced the notion that government needs to spend less energy on calculating how to punish unauthorized disclosures of politically sensitive information to the news media and more on distinguishing the truly sensitive information which must be protected. Once that information is identified as properly warranting protection, government officials and the news media have shown a willingness to honor reasonable requirements.

The second issue is the question that this Congress addressed—the House addressed in 2002 when it passed the Homeland Security Information Sharing Act, which became part of the Homeland Security Act of 2004. It mandated the creation of a unique category of information, known as sensitive homeland security information, which was sensibly designed to allow this necessary sharing of information with state and local officials while withholding it from the general public.

This designation has proven difficult for the executives to implement, so difficult that in fact it went in a different direction and the mandate instead became to disperse information control authority across of broad range of executive agencies. This resulted in a disjointed and uncoordinated proliferation of sensitive but unclassified designations to protect poorly defined categories of information.

In one instance, the Department of Homeland Security drafted a draconian nondisclosure agreement designed to apply the restric-

tions on tens of thousands of federal employees and hundreds of thousands, potentially, of state and local first responders.

Although it was only enforced briefly, this NDA was more severe than NDA's effect for sensitive, compartmented information and for a variety of controls over the most sensitive intelligence information the government has.

While it has been withdrawn, it is an indicator of the extent to which there has been little progress.

Lastly, the National Intelligence Reform Act of 2004 provided another challenge which the administration found wanting. Congress provided a broad, centralized power for the new director of national intelligence and urged the new DNI to create a tearline report system by which intelligence gathered by an agency is prepared with the information relating to intelligence sources and methods is easily severed but for the report to protect such sources and methods from disclosure.

The prospect of such a tearline encouraged many observers to believe the classification system could be improved by concentrating on the guidelines for protecting well-defined sources and methods. By making the refined decisions to protect that which truly requires protection, more of the remaining information would be available for sharing within the intelligence community, as well as with state and local officials charged with homeland security responsibilities. They were naturally a benefit for the public and the press as this information, other information, was decontrolled.

Ms. HARMAN. Mr. Armstrong, if you could summarize now, we would appreciate it.

Mr. ARMSTRONG. Increasingly, officials in certain departments must greatly risk their security clearances and potentially their careers and their family's financial security in order to correct and guide public-to-public record.

It is my hope that rather than attempt to repair the present system of over-classification to the public, that the public, the news media, the Congress and the intelligence community would benefit more from the specification of rigorous and tight definitions of sources and methods in accord with the tear-line processing of intelligence in order to maximize information sharing while protecting the nation's secrets.

Ms. HARMAN. Thank you very much.

Ms. Fuchs?

**STATEMENT OF MEREDITH FUCHS, GENERAL COUNSEL, THE
NATIONAL SECURITY ARCHIVE, GEORGE WASHINGTON
UNIVERSITY**

Ms. FUCHS. Thank you.

Chairman Harman, Ranking Member Reichert and members of the subcommittee, thank you for having me appear today.

After the September 11th attacks on the United States, there were many signs that official secrecy would increase. Some of it was legitimate, out of concern about risks posed by poorly safeguarded government information. In addition, in March 2002, White House Chief of Staff Andrew Card issued a directive to federal agencies, requesting a review of all records and policies con-

cerning the protection of sensitive but unclassified information, also called SBU.

This memorandum spurred agencies to increase controls on information.

Mr. Leonard and Ms. Harman have already talked about the classification system and some of the statistics regarding that. I am going to focus on the SBU system where while we identified 28 different information labeling standards and GAO identified 56, I have heard from the Office of the Program Manager of the information-sharing environment that they have identified at least 100 different so-called safeguarding labels.

There is no way to determine how many records are labeled with these safeguarding controls, because agencies do not track their use of these labels.

When we issued our report a year ago, we identified a number of problems posed by these policies. Since that time, the Government Accountability Office and the program manager of the Information Sharing Environment themselves have expressed the same concerns. I am going to quickly list them, and my written testimony gives some additional detail.

First, there is no monitoring of the use of safeguard labels. At many agencies, there are no limits on who can put a safeguard label on the information, and, indeed, at some agencies, that means hundreds of thousands of people are able to put these labels on. There is no time limit for how long the label lasts. Few agencies provide any procedure for the labels to be removed. Few agencies include restrictions that prohibit the use of labels for improper purposes, including to conceal embarrassing or illegal agency actions. Agencies have conflicting policies on the intersection of these labels and the Freedom of Information Act, but evidence certainly suggests that these labels are used to increase withholding of information.

These labels likely increase the cost of information security, and there is no consistency among agencies about how to use these labels. So it seems likely that they inhibit information sharing.

Focusing just on the three major concerns that my organization has, the absence of reporting mechanisms for sensitive but uncontrolled markings makes any assessment of the extent to which a policy is being used difficult, if not impossible.

Because safeguarding sensitive unclassified information impacts safety, security, budget and information disclosure, all of which are important national concerns, there ought to be some sort of overarching monitoring.

Second, in order to protect the important role that public access has played in government accountability, it is important that a system for challenging the use of these labels be established.

Third, this unregulated use of safeguarding labels inhibits information sharing. Because the systems are sprawling in their scope and uncoordinated, they set up roadblocks for sharing. Lack of trust in the system likely leads to more classification, which also limits dissemination of the information.

I would like to quickly touch on what progress has been made within the government. Mr. Leonard referred to this in his statement. As you know, Congress required the president to implement

and information-sharing environment with the Intelligence Reform and Terrorist Prevention Act of 2004. Pursuant to that, the Office of the Program Manager of the Information Sharing Environment was established to assist in the development of the environment.

A report and implementation plan for the information-sharing environment was required within one year of enactment of the law. President Bush issued a memorandum on December 16, 2005 that set up this office, and specifically directed departments and agencies to standardized procedures for handling SBU.

The resulting working group completed an inventory of designations in March 2006, and there should have been a recommendation for submission to the president by June 2006 on standardization of SBU procedures. Well, it is now March 2007, and, as far as I know, that hasn't happened.

Part of the problem may be that these legislative mandates are imposed on an executive branch that does not want Congress to interfere and is not as concerned as I would hope about government accountability. And while I am reluctant to express that sort of a sentiment, the lack of willingness by the executive branch to respond is evidenced by the refusal of the Office of the Director of National Intelligence to participate in a March 2006 report by the Government Accountability Office about this very matter.

In its report, GAO noted that the ODNI, the Office of the Director of National Intelligence, declined to comment on the draft, stating that review of intelligence activities is beyond GAO's purview.

I know that we are running short of time. I am going to just quickly raise three concerns about the process. I met, along with several other people, with Ambassador McNamara, who is now the program manager, and I was very impressed by him and the work that they have done, and I think that they have done a great analysis. However, there is nothing in the process that suggests to me that we are quickly moving to standardization of SBU labels.

While they have done an analysis, they were supposed to have submitted a recommendation to the White House in January 2007. That may have occurred. If it did, it hasn't been made public, and having public review of that is absolutely critical.

Secondly, the program manager's effort is focused on information related to homeland security, law enforcement and terrorism, but this problem of SBU is far broader, and the category of information that affects our security is even broader than that.

Placement of the program manager at the Office of the Director of National Intelligence possibly limits the likelihood that a governmentwide solution will be considered.

And, finally, there just doesn't seem to be a schedule in place. They have collected and analyzed scores of information control policies, they have many ideas about how to fix the problem, but they have been perpetually behind schedule.

I am hopeful my testimony today has been helpful, and I am happy to take any questions.

Thank you.

[The statement of Ms. Fuchs follows:]

PREPARED STATEMENT OF MEREDITH FUCHS

MARCH 22, 2007

Chairwoman Harman, Ranking Member Reichert and Members of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, I am honored to appear before you today to talk about the growing problem of government secrecy and the danger it poses to our security.

I am testifying on behalf of the National Security Archive (the "Archive"), a non-profit research institute and leading user of the Freedom of Information Act (FOIA). We publish a wide range of document sets, books, articles, and electronic briefing books, all of which are based on records obtained under the FOIA. In 1999, we won the prestigious George Polk journalism award for "piercing self serving veils of government secrecy" and, in 2005, an Emmy award for outstanding news research.

In my five years at the Archive, I have overseen five audits of federal agency FOIA processing. Most relevant to this hearing is the report we issued in March 2006 entitled: "Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information."

After the September 11, 2001, attacks on the United States, there were many signs that official secrecy would increase. The attacks themselves led to a wave of legitimate concern about the risks posed by poorly safeguarded government information. Additionally, in March 2002 White House Chief of Staff Andrew H. Card issued a directive to federal agencies requesting a review of all records and policies concerning the protection of "sensitive but unclassified" information. This memorandum spurred agencies to increase controls on information. Further, during times of war or national crisis, the government's tendency to keep secrets always becomes more pronounced and pervasive. Thus, the U.S. entry into hostilities in Afghanistan and Iraq as part of the Global War on Terrorism necessarily led to an increase in the creation of secrets.

The available statistics show that since the September 11 attacks on the United States, there has been a dramatic upsurge in government secrecy. Classification has multiplied, reaching 14.2 million classification decisions in 2005, nearly double the number in 2001. Officials throughout the military and intelligence sectors have admitted that much of this classification activity is unnecessary. Former Secretary of Defense Donald Rumsfeld acknowledged the problem in a 2005 *Wall Street Journal* op ed: "I have long believed that too much material is classified across the federal government as a general rule. . . ." ¹ The extent of over-classification is significant. Under repeated questioning from members of Congress at a hearing concerning over classification, Deputy Secretary of Defense for Counterintelligence and Security Carol A. Haave eventually conceded that approximately 50 percent of classification decisions are over-classifications. ² These opinions echoed that of then-Chair of the House Permanent Select Committee on Intelligence Porter Goss, who told the 9/11 Commission, "we overclassify very badly. There's a lot of gratuitous classification going on, and there are a variety of reasons for them." ³

Alongside traditional classification are a plethora of new non statutory labels that are being applied to protect information that is deemed sensitive but unclassified. Some estimates count over 100 different so called "safeguarding" labels for records. There is no way to determine how many records are labeled with safeguarding controls, however, because agencies do not track their use of these labels.

At the same time that the indicators all started to point to increasing secrecy, the numerous investigations into the September 11 attacks on the United States each concluded that excessive secrecy interfered with the detection and prevention of the attacks. ⁴ Other reports, including one by the Government Accountability Office and

¹ Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12.

² Subcommittee on National Security, *Emerging Threats and International Relations of the House Committee on Gov't Reform Hearing*, 108th Cong. (2004) (testimony of Carol A. Haave), <http://www.fas.org/sgp/congress/2004/082404transcript.pdf>; See *id.*, (Testimony of J. William Leonard, Director of ISOO) ("It is my view that the government classifies too much information.")

³ 9/11 Commission Hearing, (Testimony of then Chair of the House Permanent Select Committee on Intelligence Porter Goss) (2003), http://www.9-11commission.gov/archive/hearing29-11Commission_Hearing_2003-05-22.htm#panel_two.

⁴ As the staff director of the Congressional Joint Inquiry on 9/11 found, "[t]he record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and informed American public. One need look no further for proof of the latter point than the heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid." Similarly, the entire 9/11 Commission report includes only one finding that the attacks might have been prevented:

one by the successor body to the 9/11 Commission, have decried the delay in establishing a workable information sharing environment.⁵

Against this background, the National Security Archive conducted an extensive audit of the actual policies used by agencies to "safeguard" information.⁶ We filed targeted FOIA requests that identified information protection policies of 37 major agencies and components. We obtained and reviewed 28 distinct policies for protection of sensitive unclassified information, many of which allow any employee in the agency to designate sensitive unclassified information for protection, but few that provide any procedure for the labels to be removed. Only a small number of policies included restrictions that prohibit the use of the labels for improper purposes, including to conceal embarrassing or illegal agency actions, or inefficiency. Further, and perhaps most troubling from a security perspective, was the remarkable lack of consistency among agencies as to how to use these labels. Most of the policies were vague, open-ended, or broadly applicable, thus raising concerns about information sharing, the impact of such designations on access to information, free speech, and citizen participation in governance. Given the wide variation of practices and procedures as well as some of their features, it is probable that these policies interfere with interagency information sharing, increase the cost of information security, and limit public access to vital information.

Further, we concluded that there are almost no incentives to control the use or misuse of these safeguarding labels. Unlike classified records or ordinary agency records subject to FOIA, there is no monitoring of or reporting on the use or impact of protective sensitive unclassified information markings. In comparison, it is useful to look to the formal classification system, which is governed by Executive Order 12958, as amended, and is managed and monitored by the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA). ISOO publishes an annual report to the President in which it quantifies the number of classification and declassification decisions, the number of individuals with authority to classify material, and the type of information that is being classified. Such reports enable the Executive Branch and Congress to monitor the costs and benefits of the classification system and to identify trends that may suggest the need to reform the system.

The absence of reporting mechanisms for sensitive but unclassified control markings makes any assessment of the extent to which a policy is being used difficult, if not impossible. Because safeguarding sensitive unclassified information impacts safety, security, budget and information disclosure all important national concerns some form of overarching monitoring of all information control would be valuable.

Nor is there a procedure for the public to challenge protective markings. For classified information, the security classification system provides precise limits on the extent and duration of classification as well as a system for declassification, including public requests for declassification. For non security sensitive information, the FOIA provides a relatively clear and user friendly process for the public to seek access to information held by the government. Sensitive unclassified information, however, falls into a black hole. Based on anecdotal information, we believe that information previously available under FOIA or on unrestricted Web sites may no longer be available to the public. Yet, there is virtually no opportunity for the public or other government personnel to challenge a decision to mark a document for protection as SBU, FOUO, or SSI. Accordingly, in order to protect the important role that public access has played in government accountability, it is important that a system for challenging the use of sensitive unclassified information markings be established at each agency or, alternatively, that FOIA procedures be adjusted to counteract the chilling effect these markings may have on disclosure under FOIA.

⁵"publicity about Moussaoui's arrest and a possible hijacking threat might have derailed the plot." Final Report of the National Commission on Terrorist Attacks Upon the United States, at 276 (emphasis added).

⁶In January 2005, the Government Accountability Office (GAO) added "Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security" to its High Risk List, stating that they were "designating information sharing for homeland security as a government-wide high-risk area because this area, while receiving increased attention, still faces significant challenges" (GAO-05-207). On December 5, 2005, the 9/11 Public Discourse Project, the successor body of the 9/11 Commission, issued its Final Report on 9/11 Commission Recommendations. Important areas on information sharing, including "incentives for information sharing" and "government-wide information sharing," received a D in the scheme of letter grade assessments.

⁷The complete audit report is available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/press.htm>.

Congress began to respond to these problems from the outset. Both the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the development of policies for sharing classified and sensitive but unclassified information. IRTPA requires the rapid implementation of an information sharing environment (ISE) to facilitate the government-wide sharing of information about terrorist threats. As the subcommittee is aware, the office of the Program Manager of the ISE was established pursuant to IRTPA to assist, in consultation the Information Sharing Council (ISC), in the development of the ISE. A report and implementation plan for the ISE was required within one year of enactment of IRTPA. President Bush issued a Memorandum on December 16, 2005, directing federal departments and agencies to standardize procedures for handling SBU information.

The President's December 2005 Memorandum setting up the office of the Program Manager contained specific direction related to the standardization of Sensitive But Unclassified (SBU) information. Specifically, Guideline 3 required each department and agency to inventory existing SBU procedures and their underlying authorities across the Federal government, and to assess the effectiveness of these procedures and provide this inventory and assessment to the Director of National Intelligence (DNI) for transmission to the Secretary of Homeland Security and the Attorney General. The working group completed an initial inventory of SBU designations in March 2006. The original schedule would have resulted in recommendations for submission to the President regarding the standardization of SBU procedures by June 2006. More than 5 years after the September 11 attacks, however, there still is no government wide plan to standardize information controls and ensure government accountability.

Part of the problem may be that these legislative mandates are being imposed on an executive branch that does not appreciate Congressional interference and does not seem concerned about government accountability. I am reluctant to express such strong sentiments, but the lack of willingness by the Executive Branch to respond to Congress's mandates is strongly evidenced by the refusal of the Office of the Director of National Intelligence to participate in a March 2006 report by the Government Accountability Office about this very matter. In its report, GAO noted that the ODNI "declined to comment on [GAO's] draft report, stating that review of intelligence activities is beyond GAO's purview."

Further, the responsibility for overseeing the development of a comprehensive plan has been shifted from office to office; it was first lodged at the Office of Management and Budget, then at the Department of Homeland Security and now in the Office of the Director of National Intelligence. Thus, despite the urgent need to better coordinate information sharing, it has taken some time for the program to find a home. Whether the ODNI is the proper home remains to be seen, especially in light of that office's unwillingness to be subjected to congressional scrutiny. Another delay was caused by the quick departure of the first Program Manager for the Information Sharing Environment (ISE) in January 2006. He was replaced by Ambassador Thomas McNamara.

I had the opportunity, along with several other open government advocates, to meet with Ambassador McNamara on November 20, 2006. Ambassador McNamara described for our group the challenges that the office of the Program Manager is facing in rationalizing the system for safeguarding records. They must obtain the cooperation of many communities of interest, consider multiple users of information, and consider the concerns of both governmental and non governmental entities. To date, they have only analyzed the problem. The November 16, 2006, Report of the Program Manager, Information Sharing Environment, indicates that the inter-agency Information Sharing Council (ISC) created to develop an implementation plan for the ISE, along with standardizing procedures for sensitive but unclassified information, has now created a Coordinating Committee which will submit recommendations for SBU standardization through the White House policy process. We were told that a recommendation would be transmitted to the White House in January 2007, but I am not aware whether this has happened or whether the recommendation will ever be made public.

For my own part, I was impressed with Ambassador McNamara's work to date, but I was not left with any strong impression that a transparent, government wide information sharing plan will emerge any time soon. First, there are many steps in the process that do not yet appear to have taken place. A recommendation has yet to be circulated for review by interested parties. Any recommendations should be made available to the public for comment. Even the general outline of a program, which was previewed to me and others in November 2006, raised several concerns about transparency, government accountability, and appropriate procedures. Once a recommendation is accepted, then an implementation plan will be necessary. It is

possible that there will need to be statutory or regulatory changes to facilitate implementation. There certainly will be budgetary issues raised by any recommendation and plan for standardization.

Second, the focus of the Program Manager's effort is solely on information related to homeland security, law enforcement and terrorism. The problem of sensitive unclassified information is far broader, and even the category of information that affects our security is likely more extensive than is covered by the Program Manager's mandate. Placement of the Program Manager at the ODNI further limits the likelihood that a government wide solution will be considered or emerge as an outgrowth of the process. Because of the placement within the ODNI, the program manager is likely to face great challenges in implementing an information sharing network that includes agencies outside the intelligence community. Issues of information security, information sharing, and public access to information should not be addressed in a piecemeal manner. There are best practices in some agencies that should be shared, as well as lessons to be learned about the costs and benefits of secrecy and disclosure. If the problem of information controls interfering with information sharing is ever to be solved, it will require a government wide commitment.

Third, there does not appear to be any schedule in place for moving the process forward. The fact that the Program Manager has collected and analyzed scores of information control policies is progress. That analysis surely offers insight into what works and what does not. Now the analysis must be translated into a plan with strict deadlines and funding in order to make implementation a reality. Given that the project has been perpetually behind schedule, there is cause for concern about the development of an actionable plan and implementation.

Unnecessary secrecy has been on the rise since September 11, with the result of threatening our safety and national security while impeding the process of democracy and the effective functioning of government. There is no time for turf wars or bureaucratic inertia. We are long overdue for solving the challenges of information sharing and overcoming the strain on government accountability brought about by excessive secrecy. SBU designations have been noted by government authorities as a major impediment to information sharing, yet no solution to the problem has been developed. I am hopeful that my testimony today offers a rationale and a sense of urgency for instituting stronger measures to encourage needed reforms in information control programs across the federal government. I am grateful for your interest in these issues and am happy to respond to any questions.

Ms. HARMAN. I thank the three witnesses. Your testimony is very helpful.

And, Mr. Leonard, nobody doubts your good faith and hard work, but I do question whether we are making much progress rolling a big rock up a steep hill.

Let me start there. As I said, I spent 8 years on the House Intelligence Committee, and I spent many years on virtually every security committee in this House since being elected in 1992. I do respect the need to protect sources and methods. I have never, so far as I know, ever compromised a source or a method, and I understand that real people die if that happens, and we close down our ability to get sensitive information in the future, so we should never do that.

But that is the purpose of our classification system. The purpose of our classification system is not to deprive the public of information it should have, and, surely, it is not to deprive our first preventers on the ground of information they need to know what to look for and what to do.

Does anyone disagree with what I just said?

Mr. LEONARD. Absolutely not, Madam Chair.

Ms. HARMAN. I am sure you don't.

I also share Ms. Fuchs's opinion of Ambassador Ted McNamara, with whom I have met. His title is program manager, Information Sharing Environment, and he reports to the director of national intelligence, Mike McConnell. He is a good man, and he is trying to

shift a lot of information out of the classification system into this SBU system.

But, again, I am worried that we are just going to replace one protection system with another protection system.

Does anyone disagree with that thought?

No. Okay. Well, now I am really getting discouraged.

So where do I come out? I am intrigued by Mr. Armstrong's suggestion at the conclusion of his testimony—and I know I was rushing you, but I am trying to be fair all our members and here and to our second panel. I think what you said is, we need to start over. We can't take this jerry-rig system and fix it. It is too complicated, and we aren't going to fix it, we are just going to move the boxes around. We really ought to think through what our goals and objectives are and start over.

Is that what you said?

Mr. ARMSTRONG. Precisely. That is the lesson of 50 years of national security controls, 35 years since the Pentagon Papers, 34 years since Watergate and 22 years, 25 years of these three commissions that have ensued. All have come back to the same thing: If we want to protect important information, we must identify it, isolate it, understand why it needs to be protected and communicate that to government employees. They will respect it, the press will respect it, in turn, and you will not have dangerous leaks of national security information.

You will also have an enormous amount of information that is not contained in those categories that will freely available for public policy debate and discussion. That is what we need.

Ms. HARMAN. Well, let me ask the other two witnesses to respond to this innovative and, I think, potentially visionary suggestion. I am not sure we are up to this, but I just want to ask what you think about it. It is basically to start over, to identify what we need to protect.

And, as I heard you, Mr. Armstrong, you were saying if we do this right, then we actually discourage and stop leaks because information that should be in the public domain gets there, and we should presume we have patriots in our press corps who work for government, who serve in Congress and elsewhere who will protect secrets that they understand clearly need to be protected.

So my question, let's start with you, Mr. Leonard, is, what do you think about this idea of starting over to isolate what truly needs to be protected?

Mr. LEONARD. Well, clearly, the challenge of over-classification, as I included in my prepared testimony. As long ago as the 1950s, the Wright commission, established by Congress at the height of the Cold War, found that over-classification was a threat to national security.

The largest problem, as I see, with the current framework is that it is tilted toward encouraging people to withhold. Everyone is very mindful of the fact that they can be disciplined, fired, maybe even criminally prosecuted for unauthorized disclosure. Even though the policy makes an affirmative—at least the classification imposes an affirmative responsibility on cleared individuals to challenge inappropriate classifications, quite frankly, I am never aware of that ever happening.

And, to me, it is the flipside of the coin: Yes, we have to hold people accountable for inappropriate disclosures, but unless we similarly have a system to hold people accountable for inappropriate withholding or hoarding of information, the system will remain dysfunctional.

Ms. HARMAN. Thank you very much.

My time is expiring, so, Ms. Fuchs, if you have any comments, please make them now.

Ms. FUCHS. Right. I mean, I would second what Mr. Leonard said. I think that the secrecy is a reflexive response by people within the government, and it is going to be hard to fight that. There should be better training, and the incentives have to be changed. And the incentives are changed, I think, by doing oversight, having audits of secrecy decision making, making legal remedies available to the public, having whistleblower protection and having leadership on the issue.

Ms. HARMAN. Thank you very much.

The chair now recognizes Mr. Reichert for 5 minutes.

Mr. REICHERT. Thank you, Madam Chair, and, again, thank you for being here this morning.

Mr. Leonard, you made a statement, I think it was you, that said that trained people only get it right 64 percent of the time. Why is that?

Mr. LEONARD. It harkens back to the point I just made, Mr. Reichert. I was in a similar forum with a very senior official from the Defense Department once and she indicated, I think, a very prevalent line of thought, and that is, especially in time of war, people want to err on the side of caution.

And I am dumfounded by that approach, because, first of all, I never understand why we want to have error as part of any implementation strategy. But besides that, if we are ever going to get it right, to me, in time of war is the time we have to get it right.

As Ms. Fuchs says, we have to change the incentives and have people recognize that the inappropriate withholding or hoarding of information can have just as much as a deleterious impact on the national security as any unauthorized disclosure can.

Mr. REICHERT. Mr. Armstrong, would you say that that is true? In your statement, you mentioned sensitive homeland security information for state and locals don't get to the state and locals. Is that part of the problem that Mr. Leonard is talking about?

Mr. ARMSTRONG. I believe it is. I think there are two reasons. One is the bureaucratic default to caution, that it is easier to control than it is to release. But, secondly, control has its own value and purpose. It allows a manipulation of the debate. It prevents people from having a more open and participatory discussion about the allocation of resources, about priorities.

We heard in the dialogue from the Department of Homeland Security at one point that they were considering the prosecution or restraint on journalists publishing information about chlorine plants and their danger in metropolitan areas. Now, the plant doesn't become more dangerous because there is a publication of it. It is possible that some terrorist might learn that there is something there that they could blow up, but it is unlikely that they haven't already identified it.

What happens is the public learns about it, and as that information is openly discussed, precautions are taken, political actors are held accountable, and those political actors who become decisions makers during crisis begin to take appropriate action.

Mr. REICHERT. Now, for all three of you, there has been—Mr. Armstrong, you especially mentioned that you have been involved in discussions with just about every member of the intelligence community. I didn't hear you say that state and local agencies were involved in discussions that you were having. Did I incorrectly—

Mr. ARMSTRONG. No, that is correct. Our primary purpose was when the equivalent of an Official Secrets Act was passed in the year 2000 and the vetoed and then came up again the following year, we wanted to learn, in the press, we wanted to learn what the concern was in the federal government and how we might best meet that. But we have not had that discussion at the local level.

Mr. REICHERT. For all three of you, quickly, state or local public disclosure laws, have you been trying to connect with state officials and local officials to find out how to work through that problem?

Ms. FUCHS. If I could respond, I wanted to mention (it is a big problem what happens at the state and local level, and there is going to have to be some coordination. I wanted to draw the subcommittee's attention to a report that was done by the American Society of Newspaper Editors that was released last week where they did an audit where they went to state and local offices to get copies of the Comprehensive Emergency Response Plan in each of those places.

That is something that is mandated to be made public by the Emergency Planning and Community Right to Know Act of 1986, and it is something that, for instance, tells you escape routes that the public should be aware of if something happens in their community.

More than a third of the public officials refused to provide the report. It is sort of the opposite of—a variation on the story that you told, Mr. Reichert at the outset—

Mr. REICHERT. Yes.

Ms. FUCHS. —about not sharing information.

But it is the kind of thing, for instance, I know that in D.C. that K Street divides which way you get out of the city if something happens. Well, I work on one side of K Street and my kid goes to school on the other side of K Street. Knowing that information is important to me as a member of the public.

Mr. REICHERT. Yes. I would make one last point. We can come up, devise the greatest system in the world, which we don't have right now, obviously, but if we start over, it could hopefully end up being better, but the system is made up of people, and that is going to be our major problem.

I know on a number of occasions in my 33 years in the sheriff's office we were going to serve a search warrant and I showed up at an address to serve a search warrant on a suspect in that major serial case I was talking about earlier only to find a reporter standing on the front porch waiting for me. So we can build a great system, but it all boils down to the people and the responsibility that they take.

Thank you. I yield.

Ms. HARMAN. I thank the ranking member for yielding.

The chair now recognizes Mr. Langevin for 5 minutes.

Mr. LANGEVIN. Thank you, Madam Chair.

I want to thank our witnesses for testifying here today.

Can you just walk me through the process of how people get access to this sensitive but unclassified information? Does this come down to the fact that we needed better information-sharing environment among people like law enforcement, and one of the things I know that DHS is struggling through right now is creating an information-sharing environment for terrorism-related issues, similar to the type of information sharing that law enforcement—that type of a system that law enforcement has right now.

For example, in New England, we have RISNet, Regional Information Sharing Network, so that information on law enforcement issues can get out there to those that need it. DHS is struggling with creating that kind of a system. I think Charles Allen at DHS is doing a very good job of moving in the right direction, but we are certainly not there yet.

So is that the model that we have right now? I just want to get an understanding of when something is sensitive but unclassified, can anybody in the law enforcement realm—you know, is that in the need-to-know category?

Mr. LEONARD. Although not in my official realm of responsibilities, I can address that and that is the bottom line. The challenge is, there is no one model. With over 100 types of systems, I dare say there is no one individual in the entire federal bureaucracy who knows how to leverage access to all these types of controlled information.

And the challenge then, of course, is, when agencies want to leverage technology to help disseminate this information, and there are all different types of controls and constraints on it, you are somewhat restricted in terms of what you can put into a technology system if you don't know the rules for handling and disseminating and access, because there currently are no systems. And this is what Ambassador McNamara's office is in fact trying to address.

Mr. ARMSTRONG. One issue you might consider, congressman, is the fact that the Department of Homeland Security does not seem to have a risk assessment matrix that allows them to put value on particular information and figure out what it is they are trying to control and from whom.

When they issued, in 2004, a nondisclosure agreement, which I included a copy of, attached to my statement, they included the long list of things and then the words, "and other identifier used by other government agencies to categorize information as sensitive but unclassified," and gave authority to any supervisor to create any such category. So people have millions of different interpretations.

It requires leadership, it requires some identification of what the dangers are and what the purpose of controlling information is. If they can't identify that, don't control it.

Mr. LANGEVIN. Let's kind of elaborate on that, if we could, a little more. How might we go about creating a standardized system for sharing sensitive but unclassified information? And would a standard approach be a net positive? And furthermore, to what extent

do you think there will be any resistance to such an effort and from whom?

Ms. FUCHS. Well, I think that standardizing would be a benefit. I mean, we see it in the classification system, there is some regularity, there are reporting requirements, there is way to challenge classification decisions. It may not happen that often, but at least there is some transparency to the system and there is some control.

What is happening in the SBU system is it is all over the place, and the absence of any type of regulation means that it is an interference with information sharing.

But I want to also add that part of making information sharing work means including the public in information sharing, because the public has just as much concern as the government in protecting ourselves.

I mean, we all know the story of the sniper in Washington, D.C. It was only because the license plate on that car got out and a trucker who stopped at the side of the street saw the car and reported it. The public has a role to play as well, so any kind of system should consider the importance of sharing information with the public.

Mr. LEONARD. And being a lifelong bureaucrat, I find rules can be empowering as well. Because, right now, with the mass confusion, people on the frontlines and the federal bureaucracy who have to make decisions, there is such confusion that the default is, well, I don't know if I am going to default.

If we have clearly articulated rules, that can be empowering as well, because then it removes the uncertainty in people's minds. They know exactly what they can disclose, under what circumstances and who. And also then if people want to challenge those controls, we know what it is we are challenging.

Mr. ARMSTRONG. I think the standardization needs to be of the risk assessment process and of the process of engaging the partners with whom you want to share information. If you build it, they will come, but it has to be truly understood, as Meredith mentioned, those partners include the public. The chlorine plant situation, people who own chlorine plants do not want information distributed about them, particularly when there are risks from them.

Ms. HARMAN. The time of the gentleman has expired.

The chair now recognizes the very patient Mr. Dent of Pennsylvania for 5 minutes.

Mr. DENT. Thank you, Madam Chairman.

Mr. Leonard, the president directed that the designation of sensitive but unclassified information be standardized. In response, an interagency working group, led by DHS, DOJ and the program manager for the Information Sharing Environment, initiated an effort to address these issues. I understand that your office is part of that effort and that the working group has submitted recommendations to the president regarding the standardization of sensitive but unclassified procedures.

When do you expect these recommendations to be approved by the president? And what outstanding issues are there?

Mr. LEONARD. Sure.

Congressman I serve as an advisor to the working group that Ambassador McNamara heads up. Being an observer and an advi-

sor to that group, I can attest that significance progress has been made. Those recommendations actually have not yet been passed up to the president as of yet, but my understanding is that the timeline is a matter of months of get it through the process.

Mr. DENT. To get it to the president.

Mr. LEONARD. To get it to the president; yes, sir.

Mr. DENT. Okay. Then what can we do to assist you through this process? I mean, what can Congress do?

Mr. LEONARD. Well, one of the challenges that I have always took note of is that many of the controls that agencies have placed on unclassified information are actually based in statute. And one of my observations has been is that each and every time we create one of these new homegrown controlled items, that we seem to do it from scratch and we don't pay homage to what has gone before.

And I believe whenever Congress makes the observation that certain types of information needs to be controlled from a statutory point of view, that to whatever extent including in those mandates is the need to ensure that it is being done in a consistent manner, I think would be highly effective.

Mr. DENT. More specifically, Mr. Leonard, I know you testified before that the classification authority is pursuant to the president's article 2 authorities under the Constitution, and that certainly complicates these legislative remedies.

So, I guess, what, in your opinion, would a legislative remedy to the problem of over-classification and pseudo-classification look like?

Mr. LEONARD. Well, my reference to the president's article 2 authority, of course, is with respect to the classification for a national security information system, which I oversee. The pseudo-classification system, as I said, that has its origins in a number of different areas.

Anything that we can do to change—the observation was made about ultimately it is people who make the system works, and anything that we can do to encourage people to recognize the need that inappropriate withholding of information is similarly deleterious and change that culture is, I think, ultimately what is required in this area.

Mr. DENT. Thank you.

And, finally, in August of 2004, you testified, essentially, that the creation of a director of national intelligence would be a good thing if the DNI could overcome all of the nuances in the classification system.

Has this been the case, or does the DNI need more authorities to iron out the classification system, in your opinion?

Mr. LEONARD. The DNI has taken a leading role, from my observation, in terms of trying to establish greater consistency with respect to how the intelligence sources, methods and activities are handled across the board. That is obviously a work in progress, but my observation is that the DNI has taken a much needed leadership role in this area.

Mr. DENT. Thanks, Madam Chairman. I yield back.

Ms. HARMAN. I thank the gentleman.

As this panel exits, I would just like to note that I was one of the godmothers for the creation of the Department of Homeland Se-

curity, and I was a coauthor of the legislation establishing the Office of the Director of National Intelligence, and our clear intent, on a bipartisan basis, was to simplify, not complicate, this system.

So I am hopeful that this subcommittee, on a bipartisan basis, will take up Mr. Armstrong's challenge and see if we can accomplish that goal, which is a lot later than we intended but very timely.

The first panel is excused, and as the second panel comes up, I would note that we are expecting votes between 11:15 and 11:30. Mr. Reichert and I want to hear from both witnesses and ask our questions very promptly, because we don't want you to have to stay around for the half hour or more that we will have to recess.

Thank the witnesses very much.

Okay. Let's have the second panel takes your seats. Even without nametags, we know who you are.

Our first witness, Cathy Lanier, is the chief of the Metropolitan Police Department here in Washington, D.C. She was named police chief by D.C. Mayor Adrian Fenty and assumed her position on January 2nd of this year. Before her appointment, she was tapped to be the first commanding officer for the police department's Office of Homeland Security and Counterterrorism, which was established in 2006.

A highly respected professional in the areas of homeland security and community policing, Chief Lanier took the lead role in developing and implementing coordinated counterterrorism strategies for all units within the Metropolitan Police Department and launched Operation TIPP, which is D.C.'s Terrorist Incident and Prevention Program.

Our second witness, Michael Downing, serves as the assistant commanding officer, Counterterrorism Criminal Intelligence Bureau, where he assists two regional operations, which command the Los Angeles Joint Regional Intelligence Center, called the JRIC.

And we welcome him from L.A.

I will skip all the rest of his wonderful credentials, because we want to get right to your testimony.

And, without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize as quickly as possible, starting with Chief Lanier.

**STATEMENT OF CHIEF CATHY L. LANIER, METROPOLITAN
POLICE DEPARTMENT, WASHINGTON, D.C.**

Chief LANIER. Thank you. Good morning.

Chairman Harman, members of the committee, staff and guests, thank you for this opportunity to present this statement on the impact of over-classification on information sharing.

To begin, I emphasize the important role that local law enforcement plays in homeland security efforts. We are more than merely first responders, as you have stated. We are first preventers who are uniquely positioned to detect and prevent terrorist incidents right here in our home. There are 800,000 law enforcement members across the nation who know the communities they serve and are in the best position to detect the investigative criminal activity that might be connected to terrorism.

Information provided by local police, if discovered early and matched with the right intelligence, can help detect, disrupt and prevent a terrorist plot. However, in order for local law enforcement to perform its critical role of first preventer, it is essential that the police officers and support personnel be provided with timely intelligence information. This requires an intelligence conduit consisting of an organized, effective and trusting flow of information between local law enforcement and our federal partners.

It is important to note that in the national capital region, the flow of information among our federal partners is fairly good through the JTTF. Part of that reason for that is that our agencies have worked together for years sharing information and coordinating responses to a variety of situations. Pre-established relationships and a track record of trust has made smooth and eliminated obstacles experienced by other jurisdictions. The JTTF understands local law enforcement and appreciates the value of those relationships.

Nonetheless, several issues remain as it relates to federal and local information sharing. Law enforcement needs better access to federal intelligence information as well as an enhanced ability to translate such information into local law enforcement activity. This involves classifying information appropriately as well as creating a more efficient local access, both classified and non-classified information.

Access to federal intelligence information remains a major obstacle for local law enforcement. While the security classification system that mandates security clearances helps to ensure that sensitive information is protected, it also hinders the local homeland security efforts.

Information collected by the federal government is sometimes overly classified and causes valuable information that should be shared to remain concealed. Law enforcement does not need to know the details about where information originates or how it is collected; however, we do need sufficient and timely information in order to know what to look out for as well as what scenarios to prepare for.

Information provided by the federal government that is dated or only shared once the threat becomes imminent does not offer value to local law enforcement. At this point, it is too late for us to enhance our capabilities to effectively deal with a threat. Conversely, local law enforcement analysts should also ensure that intelligence they collect is assessed and shared with DHS, FBI and other local and state agencies.

The significant challenges facing local law enforcement is in translating this intelligence once it is obtained from the federal government into actions for local jurisdictions. This challenge is notably exacerbated when the information provided is either not timely or is restricted so that it cannot be shared with other stakeholders.

It is critical that the local law enforcement community be made aware of global trends regarding people and organizations that have a potential to commit crimes or pose a bona fide threat to our community. Awareness of these global trends will identify emerg-

ing threats and allow me to properly train my patrol officers on the individual elements needed to mitigate these emerging threats.

As a police chief, I need various forms of intelligence that will come from a variety of different agencies. On the strategic side, I need a global view of known terrorist organizations, groups and individuals, both foreign and domestic, and the potential threat they may post to the homeland. This type of intelligence provides me with a better understanding of the history of these groups, their capabilities and their interest in particular targets or weapons.

The broad nature of this type of intelligence, in my opinion, should not be classified beyond law enforcement sensitive. Even when it involves emerging groups and capabilities, as long as the information remains in the law enforcement community and is used for legitimate law enforcement purposes, it should not cause harm to any ongoing intelligence operation.

In addition to increased awareness of global trends, I also need to be familiar with the local threat environment right here in the national capital region. Being familiar with the presence of known terrorist organizations in this region allows me to educate and train my officers on the known tactics used by these organizations so they can pay particular attention to the certain subtle activities while on routine patrol.

For example, if it is known that a particular terrorist organization that has a presence in the NCR is known to engage in financing terrorist activities by selling unpacked cigarettes, my patrol officers need to be aware of this so that particular tactic—so they would know which information needs to be shared with the JTTF for further analysis.

This intelligence, combined with information such as how these groups travel, communicate and influence will help me influence the resource allocation, training, prevention efforts and response practices.

The bottom line, the frontline officers who see individual elements of crimes every day need to be knowledgeable of emerging threats and tactics in order to link these individual elements so that trends can be identified early and mitigated quickly.

I will skip to the end of my testimony to stay within the time, but I do believe that ultimately improvements in the intelligence-sharing environment will make our nation safer, as the federal government and local first responders work jointly as first preventers.

And I thank you for having this opportunity today.

[The statement of Chief Lanier follows:]

PREPARED STATEMENT OF CATHY L. LANIER

MARCH 22, 2007

Chairwoman Harman, members of the Committee, staff and guests—thank you for the opportunity to present this statement on the impact of overclassification on information sharing. Specifically, I will address federal level information sharing with local law enforcement.

To begin, I emphasize the important role that local law enforcement plays in homeland security efforts. We are more than merely first *responders*. We are first *preventers* who are uniquely positioned to detect and prevent terrorist incidents right here at home. There are 800,000 law enforcement members across the nation who know the communities they serve and are in the best position to detect and investigate criminal activity that might be connected to terrorism. Information pro

vided by local police if discovered early and matched with the right intelligence can help detect, disrupt and prevent a terrorist plot.

However, in order for local law enforcement to perform its critical role of first *pre-venter*, it is essential that police officers and support personnel be provided with timely intelligence information. This requires an intelligence conduit consisting of an organized, effective and trusting flow of information between local law enforcement and our federal partners. It is important to note that in the national capital region, the flow of information among federal, state and local partners through our Joint Terrorism Task Force (JTTF) is quite good. Part of the reason for this is that our agencies have worked together for years sharing information and coordinating responses to a variety of situations. Pre established relationships and a track record of trust have smoothed many of the obstacles experienced by other jurisdictions. The JTTFs understand local law enforcement, and appreciates the value of local relationships. I believe other aspects of the federal homeland security community could learn from the experiences of the JTTFs.

Nonetheless, several issues remain as it relates to federal local intelligence sharing practices. Local law enforcement needs better access to federal intelligence information, as well as an enhanced ability to translate such information into local law enforcement activity. This involves classifying information appropriately, as well as creating more efficient local access to both non classified and classified information. Further, we need to recognize the importance of smaller law enforcement agencies, as well as the need to expand homeland security efforts beyond our traditional partners. I will discuss these issues in greater detail in this testimony.

Access to federal intelligence information remains a major obstacle for local law enforcement. While the security classification system that mandates security clearances helps to ensure that sensitive information is protected, it also hinders local homeland security efforts. Information collected by the federal government is sometimes overly *classified*, causing valuable information that should be shared to remain concealed.

Local law enforcement does not need to know details about where information originates or how it was collected. However, we do need sufficient and timely information in order to know what to look out for as well what scenarios to prepare and drill for. Intelligence analysts should assess intelligence information and synthesize it in a manner that allows pertinent information to be shared widely among local law enforcement personnel. This requires that they write the analysis for release and appreciate the type of actionable information useful to law enforcement. I want to also emphasize the importance of quickly sharing information even if the information is not fully vetted. Information provided by the federal government that is dated or only shared once a threat becomes imminent does not offer value to local law enforcement. At this point it is too late for us to enhance our capabilities to effectively deal with the threat. Conversely, local law enforcement analysts should also ensure that intelligence they collect is assessed and shared with DHS, FBI, and other local and state agencies.

A significant challenge facing local law enforcement is translating the intelligence information that is obtained from the federal government into action for local jurisdictions. This challenge is notably exacerbated when the information provided either not timely or is restricted and cannot be shared with other stakeholders. It does a local police chief little good to receive information including classified information about a threat if she cannot use it to help prevent an attack. Operationally, local law enforcement needs to be aware of the presence of possible terrorist organization activity in their jurisdiction and surrounding region. This intelligence combined with information such as how these groups travel and communicate influence local law enforcement resource allocation, training, prevention, and response practices.

It is critical that the local law enforcement community be made aware of global trends regarding people and organizations that have the potential to commit crimes or pose a bona fide threat to the community. Awareness of these global trends will identify emerging threats and allow me to properly train my patrol officers on the individual elements needed to mitigate these emerging threats. As a police chief I need various forms of intelligence that will come from a variety of different agencies. On the strategic side, I need a global view of known terrorist organizations, groups and individuals both foreign and domestic and the potential threat they may pose to the homeland. This type of intelligence provides me with a better understanding of the history of these groups, their capabilities and their interest in particular targets or weapons. The broad nature of this type of intelligence, in my opinion, should not be classified beyond "law enforcement sensitive". Even when it involves emerging groups or capabilities, as long as the information remains in the law enforce

ment community, and is used for legitimate law enforcement purposes, it should not cause harm to any ongoing intelligence operation.

In addition to increased awareness of global trends, I also need to be familiar with the local threat environment in the national capitol region. Being familiar with the presence of known terrorist groups in the region allows me to educate and train my officers on the known tactics used by these organizations so they can pay particular attention to certain subtle activities while on routine patrol. For example, if it is known that a particular terrorist group that has a presence in the NCR is known to engage in financing terrorist activities by selling untaxed cigarettes, my patrol officers need to be aware of these and other tactics so that they would know which information to pass to the JTTF for further analysis.

The bottom line issue is that the frontline officers, who see the individual elements of crimes, need to be knowledgeable of emerging threats and tactics in order to link these individual elements so that trends can be identified early and mitigated quickly.

Importantly, there are also occasions where local law enforcement officials may need to be apprised of classified information. There is no question that local law enforcement personnel have added value to federal task forces—such as the JTTFs—as well as Department of Homeland Security operation centers. It is for these reasons that appropriate security clearances must be granted in a timely manner—to local police.

While the Metropolitan Police Department (MPD) has obtained a number of security clearances for its members, that is not true for all law enforcement organizations. It is imperative that federal, state, and local law enforcement personnel that are working together to protect the nation from terrorist threats be on equal footing. While local law enforcement has seen some improvement in the process of receiving security clearances, more must be done to expedite the process.

I am optimistic that the DHS supported fusion centers that are becoming operational across the country will help bridge some the existing intelligence sharing gaps. This will be accomplished by having analysts from different agencies and perspectives talking to each other and working together.

While large sized police departments have the ability to develop and implement more sophisticated intelligence functions, small agencies are sometimes left out of the loop. In the Washington area alone there are 21 municipal law enforcement agencies that have less than 40 police officers. It is incumbent upon the federal government and large police departments to ensure that smaller agencies are kept informed and understand the importance of intelligence information. Formal liaisons should be established, and every agency no matter how small should have an accessible representative that is familiar with handling intelligence information.

I also believe that federal and local law enforcement should consider expanding its homeland security efforts beyond traditional parameters. We need to examine the possibility of establishing intelligence conduits with other local government components. Firefighters, paramedics and health workers, are well positioned to contribute valuable information to help protect our communities. In order to harness these types of resources, intelligence-sharing networks must be more inclusive. Further, the intelligence community will also need to work on developing and sharing intelligence that is actionable for other professions. We should begin planning for this new front now.

Finally, local law enforcement recognizes that in addition to needing timely intelligence from federal agencies, we also must be willing and able to share timely and useful information gathered at the local level with our federal state, and local partners. This is what the fusion center concept is all about. Local law enforcement stands ready to do its part in contributing to and receiving and acting upon the information that we hope will be shared more extensively in the future.

Ultimately, such improvements in intelligence sharing will make our nation safer, as the federal government as local first responders work jointly as first *preventers*.

Thank you again for the opportunity to appear before you today.

Ms. HARMAN. Thank you, Chief. Your testimony is very important for the hearing record.

Mr. Downing?

**STATEMENT OF MICHAEL DOWNING, ASSISTANT
COMMANDING OFFICER, COUNTER-TERRORISM/CRIMINAL
INTELLIGENCE BUREAU, LOS ANGELES POLICE DEPARTMENT**

Mr. DOWNING. Chairman Harman, Ranking Member Reichert, members of the subcommittee, thank you for the opportunity to discuss the Los Angeles Police Department's efforts to fight terrorism and the important issue of the over-classification of intelligence.

Having recently returned from an 8-week attachment to the new Scotland Yard's Counterterrorism Command, I have a much greater appreciation for change and why we need to change.

In Peter Clarke's words, the national coordinator for counterterrorism, if you looked at the 30-year IRA campaign and look at the antithesis of that campaign, that is the threat that they have now. To take a 130-year-old organization's special branch and amalgamate it into the counterterrorism command is huge change for a culturally rich institution, and if they change, we certainly need to change.

Local law enforcement's ability to play a significant role in stopping terrorism is seriously hampered by the over-classification of intelligence by the federal government. In Los Angeles, we enjoy a positive constructive partnership with various federal agencies, but the classification process has been a substantial roadblock to our capacity to investigate terrorism cases.

The terrorist threat to our communities currently involves continued domestic terrorism and international terrorists plotting to destroy American cities. Prior to September 11, local law enforcement agencies primarily investigated domestic terrorist groups, including white supremacists, hate groups, special issue groups conducting criminal activities. Investigations centered on familiar cultures that were socially motivated by political ideologies to commit terrorism.

The bombing of the Alfred Murrah building in Oklahoma, in 1995, the most notable domestic terrorist attack, had a catastrophic impact on American soil and brought together local and federal law enforcement to bring the terrorists to justice. Local law enforcement, in fact, played a critical role in the investigation and apprehension of the offenders.

I understand that you are coming to Torrance in a few weeks for a field hearing. The JIS case was an unclassified case that dealt in prison radicalization and conversion to gangs and terrorism. That was an unclassified case because it didn't have an international connection. Had it had an international connection, it would have been classified and the outcome perhaps could have been much different.

Prior to September 11, international terrorism was not in the national consciousness. Despite the first World Trade Center bombing, most Americans did not realize the significant threat of Islamic extremism and the consequences of this terrorism. September 11 changed the mindset of all Americans, including local law enforcement.

In addition, in the war on Afghanistan, and later in Iraq, the face of Islamic terrorism changed. No longer was the only threat a group of dissident Saudis hijacking a plane to crash into American symbols of power. Throughout the world, suicide bombers at-

tacked discos, train stations and buses. Islamic terrorism has continued to demonstrate its reach and power from changing the outcome of the 2004 national election in Spain to paralyzing the transportation system in London in 2005.

The terrorist transformed himself from Middle East foreigner to second and third generation local citizen.

The sheer number of terrorist threats to our communities across the country has increased dramatically, and the federal government's capacity to collect intelligence and investigate these threats has been overwhelmed. Consequently, local law enforcement's efforts to counterterrorism has never been more important and has never been more critical.

Across the country, a new concept of fusion centers arose, where analysts from police departments, FBI, Immigration and Customs Enforcement and other agencies worked on the same information screens to identify possible terrorist threats.

In Los Angeles, the LAPD provides personnel to participate in the JRIC located in Norwalk, California. We have 14 other participating agencies in that center.

The JRIC provides critical information-sharing opportunities with the federal government. However, over-classification of intelligence has become an impediment to full information sharing with the local law enforcement agencies who participate in the JRIC. As such, it has provided an impediment to the JTTFs, which is a great success story in our partnership with the federal agencies.

After the 9/11 Commission issued its comprehensive report, America's local law enforcement community, consisting of over 700 law enforcement officers, was reluctantly invited into the effort of countering the international terrorist threat. One part of the rationale was that neither the CIA or DOD could conduct intelligence operations within the U.S. against American citizens.

Moreover, the total number of FBI special agents assigned to protect over 18,000 cities, towns and villages throughout the United States is slightly over 12,000 people. This number becomes less reassuring when one examines the number of agents needed to handle the FBI's other responsibilities, including white collar crime, organized crime, public corruption, financial crime, fraud against the government, bribery, copyright infringements, civil rights violations, bank robbery, extortion, kidnapping, espionage and so on.

At the national level, local law enforcement was not deemed an important stopgap in the field of counterterrorism, particularly in the area of Islamic extremists. In addition, the significant role of—

Ms. HARMAN. Mr. Downing, could you please summarize at this point, because we are concerned that a vote will be called.

Mr. DOWNING. Thank you. I will conclude, Ms. Chairman.

The United States faces a vicious, amorphous and unfamiliar adversary on our land. Our previous defensive strategy to protect our cities was ineffective, and our current strategy is fraught with issues. We cannot support any process that takes us closer to another failure.

We have mutual interest in working common direction to prevent acts of terrorism in the United States. The classification levels are

based on fear, the probability of information being disseminated to those that can cause serious damage to national security. What this system is not designed to do is to protect us against the threat itself.

This is achieved by disseminating the information to people who stand the best chance of stopping violence against American cities, our first preventers and law enforcement.

[The statement of Mr. Downing follows:]

PREPARED STATEMENT OF MICHAEL P. DOWNING

MARCH 22, 2007

I. Introduction

Chairman Thompson, Chairwoman Harman, Ranking Member Reichert, and Members of the Subcommittee, thank you for the opportunity to discuss the Los Angeles Police Department's (LAPD) efforts to fight terrorism and the important issue of the over classification of intelligence.

Local law enforcement's ability to play a significant role in stopping terrorism is seriously hampered by the over classification of intelligence by the federal government. While in Los Angeles we have enjoyed a very positive and constructive partnership with various federal law enforcement agencies, including the Federal Bureau of Investigation's (FBI) Los Angeles Field Office and the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the classification process has been a substantial roadblock to our capacity to investigate terrorism cases and work hand-in-hand with these federal agencies.

II. The Terrorist Threat to Our Local Communities

The terrorist threat to our communities currently involves continued domestic terrorism and international terrorists plotting to destroy American cities.

A. Domestic Terrorism

Prior to September 11, local law enforcement agencies primarily investigated domestic terrorist groups, including white supremacists, hate groups, and special-interests groups conducting criminal activity (e.g. the Animal Liberation Front). Investigations centered on familiar cultures that were socially motivated by political ideologies to commit terrorism. The bombing of the Alfred P. Murrah Federal Building in Oklahoma in 1995, the most notable domestic terrorist attack, had a catastrophic impact on American soil and brought together local and federal law enforcement to bring the terrorists to justice.¹ Local law enforcement, in fact, played a critical role in the investigation and apprehension of the offenders.

B. International Terrorism

Prior to September 11, 2001, international terrorism was not in the national consciousness. Despite the first World Trade Center bombing, most Americans did not realize the significant threat of Islamic extremism and the consequences of international terrorism. September 11 changed the mindset of all Americans including local law enforcement.

Since September 11, the scope of terrorism and extremism has increased exponentially. In addition, as the war in Afghanistan and later in Iraq waged on, the face of Islamic terrorism changed. No longer was the only threat a group of dissident Saudis hijacking a plane to crash into American symbols of power. Throughout the world, suicide bombers attacked discos, train stations, and buses. Islamic terrorism has continued to demonstrate its reach and power from changing the outcome of the 2004 national election in Spain to paralyzing the transportation system in London in 2005. The terrorist transformed himself from Middle East foreigner to second and third generation local citizen.

The sheer number of terrorist threats to our communities across the country has increased dramatically and the federal government's capacity to collect intelligence and investigate these threats has been overwhelmed. Consequently, local law enforcement's efforts to counter terrorism have never been more important or critical.

III. LAPD's Response to Terrorist Threats

A. Counter-Terrorism Bureau

¹The 1993 World Trade Bombing was seen as international terrorism and investigated by the FBI.

The Los Angeles Police Department has taken the threat of international terrorism very seriously. The city has a population of over 4 million and spans over approximately 500 square miles. The region is home to numerous potential terrorist targets including the Los Angeles International Airport, the ports of Los Angeles and Long Beach, and the entertainment industry. In response, the LAPD has invested numerous hours and millions of dollars toward preparedness and response to a possible terrorist attack. In addition, the LAPD has created a Counter-Terrorism/Criminal Intelligence Bureau with nearly 300 officers who are solely dedicated to counter-terrorism and criminal intelligence gathering. While this bureau has served a critical function in the war against terror, the LAPD has been required to dedicate officers to intelligence gathering, a function typically performed by the federal government.

B. Joint Regional Intelligence Center and Joint Terrorism Task Force

Across the country, a new concept "fusion centers" arose where analysts from police departments, the FBI, Immigration and Customs Enforcement, and other agencies worked on the same information streams to identify possible terrorist threats. In Los Angeles, the LAPD provides personnel and participates in a Joint Regional Intelligence Center (JRIC), located in Norwalk, California, which includes fourteen participating agencies. The JRIC provides a critical information sharing opportunity with the federal government. However, the over classification of intelligence has become an impediment to full information sharing with the local law enforcement agencies who participate in the JRIC.

The LAPD, as well as other Los Angeles area law enforcement agencies, is an active participant in the Joint Terrorism Task Force (JTTF). Like the JRIC, the JTTF also serves as an excellent partnership with federal law enforcement agencies and provides the opportunity for extensive information sharing. The same impediments of the JRIC, however, apply to the local law enforcement agencies participating in the JTTF. The dissemination of critical intelligence is restricted due to its over classification.

IV. The Consequences of Over-Classification of Intelligence

After the 9/11 Commission issued its comprehensive report, America's local law enforcement community, consisting of over 700,000 law enforcement officers, was reluctantly invited into the effort of countering the international terrorist threat. One part of the rationale was that neither the Central Intelligence Agency nor Department of Defense could conduct intelligence operations within the United States against American citizens. Moreover, the total number of FBI Special Agents assigned to protect over 18,000 cities, towns, and villages throughout the United States is slightly over 12,000. This number becomes less reassuring in the when one examines the number of agents needed to handle the FBI's other responsibilities including white collar crime, organized crime, public corruption, financial crime, fraud against the government, bribery, copyright infringement, civil rights violations, bank robbery, extortion, kidnapping, espionage, interstate criminal activity, drug trafficking, and other serious violations of federal law.

At the national level, local law enforcement was not deemed an important stopgap in the field of counter-terrorism particularly in the area of Islamic extremists. In addition, the significant role of local law enforcement in the fight against international terrorism was not viewed as significant. More than five years after the tragic events of September 11, local law enforcement involvement has still not been fully embraced because of the impediment of information sharing and the over classification of intelligence.

The result of including local law enforcement is that uniform police officers, bomb squads, and hazardous material teams now train together to address terrorist threats with the FBI, Department of Energy, Federal Emergency Management Agency, and the Department of Homeland Security, and train to respond to possible terrorist scenarios.

Local law enforcement has had a long history in investigating individuals and groups while developing and handling human and electronic intelligence. No agency knows their landscape better than local law enforcement; it was designed and built to be the eyes and ears of communities. Over classification, however, prevents a true partnership with federal agencies.

An impediment for both federal and local agencies, for example, is that local FBI agents, cannot change the originating agency's classification level, and this problem is amplified when the response to the threat is time sensitive. Appropriate law enforcement response to substantial threats can be significantly impaired with minimal lead time, creating greater risk to the community, and impacting the ability for a "First Preventer" response. A local field agent, however, has the discretion to classify a case as "secret." The criteria for this classification is "secret shall be applied

to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security." Additionally, the standard used for "secret" for intelligence information is "the revelation of significant intelligence operations." Many field agents may over-classify their cases for fear of compromise. Unfortunately, this is a double edge sword because it stifles collaboration with local law enforcement.

The burden to overcome is that the investigations push up against federal investigations, which in turn become classified. The result is the old adage of local law enforcement pushing information to federal agencies without getting anything back. The federal fix has been to brief the Chief of the executive staff of classified cases, but restricted the dissemination to their intelligence units (despite proper clearance levels of personnel). The result is to develop separate and likely redundant intelligence gathering operations. For example, New York was first in the country to disengage from relying on the federal agencies to protect their city, committing almost 1,200 officers to counter terrorism efforts. Currently, the association of Major Cities Chiefs of Police is campaigning in Congress to send police officers overseas to obtain information from their police counterparts rather than rely on our own federal agencies to share information.

V. Recommendation

The declassification of information currently classified at the secret level would greatly improve the information-sharing environment and build upon the counter-terrorism capabilities of local law enforcement. Federal authorities should consider changing the criteria classification of terrorism-related intelligence to "Law Enforcement Sensitive" to enable the dissemination of information to critical personnel in the field. "Top Secret" should be an exceptional classification that requires extraordinary demonstration of need while "Secret" should be a classification that requires more stringent demonstration of need than currently required.

Local law enforcement already works in an environment with a "right and need to know" and efforts made to declassify "secret" information to "law enforcement sensitive" would not only make for more effective and timely intelligence, but inspire true partnership, better collaboration, the building of more robust trust networks, and develop a richer picture with regard to community intelligence.

VI. Conclusion

The United States faces a vicious, amorphous, and unfamiliar adversary on our land. Our previous defensive strategy to protect our cities was ineffective and our current strategy is fraught with issues. In Los Angeles, we cannot support any process that takes us closer to another failure. We have the mutual interest and are working in common direction to prevent acts of terrorism in the United States. The classification levels are based on fear: the probability of information being disseminated to those that can cause serious damage to national security. What this system is not designed to do is protect us against the threat itself. Local law enforcement has a culture and capacity that no federal agency enjoys; the know how and ability to engage a community and today it is a vital part of the equation. This is achieved by disseminating the information to people who stand the best chance of stopping violence against American cities: our first preventers in local law enforcement.

Ms. HARMAN. Thank you very much.

The chair now recognizes the chairman of the full committee, the gentleman from Mississippi, for 5 minutes of questions.

Mr. THOMPSON. Thank you very much, Madam Chairman. I appreciate the opportunity.

Chief Lanier, nice to see you again. You do us proud.

Chief LANIER. Thank you.

Mr. THOMPSON. Mr. Downing, New York City saw that they had a problem with cooperation and communication with respect to intelligence. So they created their own intelligence division to kind of address many of the items you shared with us today.

What has the Los Angeles Police Department put together to address some of the issues that we are talking about today?

Mr. DOWNING. We have our own intelligence section as well, probably 30 people dedicated to gathering intelligence within our major crimes division, which does not include the Joint Regional Intelligence Center.

The Joint Regional Intelligence Center sits on top of seven counties that the L.A. FBI office is in charge of. We have approximately 44 people in that center, growing to 80. It is going to be a 7-day, 24-hour operation. It is an all crimes, all hazards approach to intelligence. However, with the minimal staffing right now, it is primarily terrorism. But that is how we deal with it.

The FBI has established that as a top-secret level JRIC center. It is managed by the L.A. sheriffs, LAPD and the FBI, with the FBI as the functional lead in the center.

Mr. THOMPSON. Thank you, and I will get back to the other part.

Chief Lanier, do you believe that you are receiving all the information, or your department is receiving all the information necessary from federal government sources at this point?

Chief LANIER. No, I am sure I am not.

Mr. THOMPSON. And without pointing fingers, can you tell me who is good, who is not so good, who is deserving of being better? Because what we are trying to do with the hearings is trying to determine where we need to start to focus. For instance, I will give you a good example, our Capitol Police happen to use analog radios. Well, they can't talk to anybody but themselves, because everybody else is digital. And that is a problem. So if we can't talk to each other from an interoperability standpoint, I am wondering how much of the sharing of intelligence and other things.

So if you could kind of give me your analysis of what you have found so far.

Chief LANIER. I can walk that fine line there, sir.

Mr. THOMPSON. All right.

Chief LANIER. First of all, I always believe if I am going to criticize anybody for anything, we have to look at ourselves first. And I will say that local law enforcement needs to do a better job of clearly articulating what our intelligence needs are to the various intelligence agencies so they know what to give us.

It took some pushing from me—fortunately, I had the support from Chief Ramsey—to go to the right people and the right agencies and say, "This is what I need and why I need it." It is not enough to say, as a police chief, "You are not giving me enough information; give me more."

If the other federal agency doesn't know what it is that I need, they are going to give me what they think I need. So I need to lay that out very clearly. So we are guilty as well.

With that said, now I can throw other stones. I do think that the participation of the JTTF has increased the information-sharing flow with the FBI because there is a longstanding history there. The new players in the game, through the Department of Homeland Security, does not have that longstanding relationship and well-established conduit for information to flow clearly.

And, I don't want to oversimplify this, but I think it is really, really important that in a lot of cases it boils down to the right people, in the right place, having an opportunity to sit down and have a dialogue. I would be happy to sit down with somebody in this classification issue and have them sit across the table from me, as a police chief in the nation's capital, and look me in the eyes and listen to what I have to say about what my needs are and then tell me why I shouldn't have that.

Mr. THOMPSON. You do a good job.

Chief LANIER. Thank you.

Mr. THOMPSON. Thank you very much.

I yield back, Madam Chair. Thank you.

Ms. HARMAN. Thank you, Mr. Chairman.

The chair now yields 5 minutes for questions to the ranking member, Mr. Reichert, from Washington.

Mr. REICHERT. This brings back memories to me.

Ms. HARMAN. Nightmares.

Mr. REICHERT. Yes. Everything that you have each said I struggled with as the sheriff in Seattle. And the sharing of information between the federal agencies and local sheriff's office and the local Seattle Police Department and the other 38 police departments in King County, every one of those chiefs would be saying exactly the same thing that both of the witnesses have said today.

When you talk about information sharing, of course one of the things that we know is a necessity in these days is technology.

Are either of you familiar with the LInX System?

Chief LANIER. Yes.

Mr. REICHERT. Are you participants in that program or beginning to become involved in that program or where do you stand, each of you?

Chief LANIER. We are not yet, but we are in the process of getting there. As you might have seen in some of my public testimony lately, technology is still a significant struggle for the Metropolitan Police Department. We are moving forward and bringing up our fusion center, so we are on our way, and we will be full participants in the LInX Program, so we are getting underway with that now.

Mr. REICHERT. Great.

Mr. DOWNING. Yes. And we, as well, are beginning in that process. We have cops LInX, which connects the agencies within the different counties, and some of the counties that can't afford it are not participating but looking forward to the installation of LInX, which will also bring in the federal system.

Mr. REICHERT. Yes. Who is the lead on the LInX Systems in your areas?

Mr. DOWNING. Chief Baca, Chief Bratton, Chief Corona, from Orange County.

Mr. REICHERT. Who from the federal government, do you know?

Mr. DOWNING. Well, Steve Tidwell in the L.A. office is assisting us with that.

Mr. REICHERT. I just visited your fusion center a couple weeks ago.

Chief?

Chief LANIER. In Washington, D.C., it is being coordinated through the Council of Governments, the COG, which is regional.

Mr. REICHERT. How big is your department?

Chief LANIER. We will be at 3,900 by the end of this year and probably 4,200 by the end of next year.

Mr. REICHERT. How many people are assigned to homeland security?

Chief LANIER. You are going to get me in trouble with my local constituents, but I will tell you.

[Laughter.]

I have approximately 30 in the Office of Homeland Security and Counterterrorism, but I do have a Special Operations Division that is 225, 230 people, and I am about to merge those two units together so that every member of the Special Operations Division will now take part in that.

Mr. REICHERT. And other than UASI money, are you getting any federal assistance, grant monies to pay for those bodies?

Chief LANIER. To pay for those bodies?

Mr. REICHERT. Yes.

Chief LANIER. Now you are really going to get me in trouble.

Mr. REICHERT. I know the answer to that one, so go ahead.

[Laughter.]

Chief LANIER. There are a variety of grant funds under the homeland security program, LETPP, as you know, and the state funds as well, the UASI, but we struggle to get sometimes reimbursement for federal duties that involve dignitary protection and things—

Mr. REICHERT. You have some unfunded mandates.

Chief LANIER. Yes.

Mr. REICHERT. Yes.

Mr. Downing?

Mr. DOWNING. Yes. Our department is 9,500. We have just under 300 assigned to the Counterterrorism Bureau, which is primarily the terrorist-related matters. We are one of the six tier one cities in UASI. This year's UASI allows us to get 25 percent of the total grant toward personnel costs.

Mr. REICHERT. Okay. I have no further questions.

I yield. Thank you.

Ms. HARMAN. I thank the ranking member, and I have a few questions.

First, I want to thank both witnesses for excellent testimony.

Our goal in this session of Congress is to put ourselves in your shoes to think about what are the opportunities and frustrations of our local first preventers and how can we make the sharing of information with them and the tools that they need more effective? Because if you can't do your jobs well, we can't protect America. It is that simple.

It is not all in Washington, D.C. I know that may come as a shock to a few folks, but it is not all here.

And vertical information sharing has to be adequate, and horizontal information sharing at the local level has to be adequate too. And that is another issue that neither of you raised today but it is something that has been raised by prior witnesses.

Both of you provided some useful information.

I am quite horrified to think, Mr. Downing, that if the information about that cell in Torrance had had some international connection, we might have missed the whole thing.

That gets my attention, because in a couple of weeks when we are in Torrance, California, congratulating the Torrance PD for excellent local police work, we are going to talk about how devastating could have been attacks by a homegrown terrorist cell living next door to some of my constituents had we not prevented them from doing anything. So I just want to observe that.

And, Chief Lanier, you make a very good point when you say it is your obligation to make clear to federal agencies what you need and why you need it. I mean, that is a job you have, and you can't just assume they are going to figure it out. In fact, they are not going to figure it out. You have to be an advocate for your own needs.

And it is in that connection that I want to ask this question. The chairman of the full committee has had a long and friendly conversation with Charles Allen of the Department of Homeland Security's Office of Intelligence and Analysis—we call it I&A—about the need for local participation either on the NCTC or connected to the NCTC. And some of us were dismayed to learn in a visit we made recently to the NCTC that the new agency about to be created, called the Interagency Threat Assessment and Coordination Group, the ITACG, might have on it one representative of law enforcement.

In questions to Charlie Allen last week, he said, "Well, maybe that will change to two or three." I clearly don't know how many members of the ITACG there will be, but I would just like to ask both of you, as consumers of necessary intelligence, what do you think about the idea of one person or maybe two or three participating in the NCTC process?

Chief LANIER. Well, it is at least a start, but I will say this: Police departments around the country have very different needs based on the jurisdictions they serve as well as the capabilities that they have.

So in the Metropolitan Police Department, a large city police department, I have a lot of capabilities that a small town police department may not have. But at the same token, that small town police department, or sheriff's department, may have some vulnerabilities and some other understandings that I don't have. So I think the representation needs to be fair and representative across the board.

State agencies, state patrol, highway patrol officers have different skills and capabilities than transit police, than urban police, than university police. So there needs to be an adequate representation.

Ms. HARMAN. Mr. Downing?

Mr. DOWNING. I absolutely agree, and to take it even further, in coming back from the U.K., they have 17 people in 17 different parts of the world, and they are growing to 21. And as New York, they have eight people in eight different parts of the world as well. We are interested in that as well, because we are not sure that the local perspective is being placed on foreign intelligence.

Ms. HARMAN. I thank you for that, and I actually share that big time. I think that information sharing has to go horizontally and vertically and that your help in designing the products that you will use is absolutely indispensable. Otherwise, they may not be useful to you.

It is your point, Chief Lanier, we have to be advocates for what we need and why we need it, so I think you should be sitting inside the room when our National Intelligence Fusion Center is developing products that you are supposed to use. And then I think our

next problem is to make sure that the classification system gets revised so that you are in a position to use them.

My time has expired. I don't want to abuse this opportunity. And I have spoken more than others.

Let me just ask either of the members, starting with Chairman Thompson, whether you have any concluding remarks.

The ranking member?

Mr. REICHERT. Thank you, Madam Chair.

I just want to, again, thank you for being here and taking time out of your busy schedule to testify. And as we have learned today and previous hearings from this information, we have a lot of work to do, and we look forward to working with you to help make our country safer.

Thank you all.

Ms. HARMAN. The hearing is adjourned.

[Whereupon, at 11:34 a.m., the subcommittee was adjourned.]

**THE RESPONSE OF THE PROGRAM
MANAGER OF THE INFORMATION
SHARING ENVIRONMENT
PART II**

Thursday, April 26, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The committee met, pursuant to call, at 10:05 a.m., in Room 1539, Longworth House Office Building, Hon. Jane Harman [chairwoman of the committee] presiding.

Present: Representatives Harman, Langevin, Thompson, Reichert, and Dent.

Ms. HARMAN. [Presiding.] Good morning. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on "The Over-Classification and Pseudo-Classification of Government Information: The Response of the Program Manager of the Information Sharing Environment."

We are here today because our classification system is broken and because pseudo-classifications are making effective information sharing nearly impossible.

A few weeks ago, we heard from experts in these areas who described an expanding problem that is making securing the homeland harder. Last fall, the president appointed Ambassador Ted McNamara to take on the pseudo-classification issue, and the ambassador has worked a solution that the White House is reviewing.

His proposed controlled unclassified information, CUI, framework holds a lot of promise, but no matter how good this solution might be, if federal agencies don't get on board, and fast, well-planned and well-meaning efforts will fail.

I commend Ambassador McNamara, with whom I have met several times, for including state and local law enforcement officers in his process from the outset. The ambassador's working group welcomed law enforcement as part of the process from day one, as well they should have.

Police and sheriff's officers are among the people who will be most affected by this new CUI framework. As all of us on the subcommittee have stated, we cannot have a successful fix to the pseudo-classification and other information sharing challenges unless all affected parties are involved in structuring the solution.

I hope that DHS is listening. You should know, and I think you do, that this subcommittee is extremely concerned with the absence of numbers of state and local participants in the new ITACG that is being developed as an adjunct to the NCTC. We think that is a problem, and we are going to stay on that problem and hopefully change what is happening.

So in this case, in addition to Ambassador McNamara and our DHS and FBI witnesses, we are joined this morning by Mark Zadra, the assistant commissioner of the Florida Department of Law Enforcement. Mr. Zadra will talk to us about the promise and potential pitfalls of the CUI framework from his state-level perspective.

I would note with sadness, however, that we are not joined today by Colonel Bart Johnson of the New York State Police, who had been invited as a witness and was originally scheduled to testify. Late yesterday, two of his officers were shot while attempting to apprehend a criminal suspect on Tuesday, and one, Trooper David Brinkerhoff, died from his injuries. Our condolences, and obviously the condolences of the entire Committee on Homeland Security, go to his family and his colleagues.

And I ask unanimous consent to enter his prepared remarks into the record at this point. Hearing no objection, we will do so.

[The statement of Colonel Johnson follows:]

FOR THE RECORD

PREPARED STATEMENT OF COLONEL BART R. JOHNSON

APRIL 26, 2007

Chairman Thompson, Ranking Member King, Chairwoman Harman, and Members of the Subcommittee, I sincerely appreciate the opportunity to appear before you today to discuss state and local law enforcement's involvement with standardizing procedures for sensitive but unclassified (SBU) information and related issues impacting local, state, and tribal law enforcement.

I have served with the New York State Police for more than 24 years, and I have over 30 years experience in law enforcement. Presently, I serve as the Deputy Superintendent in charge of Field Command. I oversee the Bureau of Criminal Investigation, the Uniform Force, the Office of Counter Terrorism, Intelligence, and the associated special details of these units. I also have the privilege to serve as the vice chair of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) Advisory Committee, the chair of the Criminal Intelligence Coordinating Council (CICC) and of the Global Intelligence Working Group (GIWG). In these capacities, I have been fortunate to actively participate in discussions relating to intelligence reform, and I have provided significant input to the federal government regarding information sharing and intelligence.

I expect that we would all agree that the current number of sensitive but unclassified (SBU) designations and the lack of consistent policies and procedures for unclassified information severely hinder law enforcement's ability to rapidly share information with the officials that need it to protect our country, its citizens, and visitors. Much progress has been made recently in addressing the classification issue by way of Guideline 3, and much of the headway is due to the leadership and efforts of Ambassador Thomas E. McNamara of the Office of the Program Manager for the Information Sharing Environment (ISE) and the other relevant federal agencies. I am gratified that I have also had the opportunity to contribute to this effort.

For many years, law enforcement agencies throughout the country have been involved in the sharing of information with one another regarding investigations, crime reporting, trend analysis, and other types of information considered law enforcement sensitive. Oftentimes, these investigations involve public corruption, organized crime, narcotics, and weapons smuggling, and they frequently involve the use of undercover operations, confidential sources, and lawful covert electronic surveillance. State, local, and tribal law enforcement agencies do not have the ability to

classify their material, and we must be assured that strict control is used when handling and distributing this type of data to ensure that the information and investigation are not compromised and that we do not sustain a loss of a life. Also, since September 11, 2001, law enforcement agencies nationwide are more fully involved in the prevention, mitigation, and deterrence of terrorism, and consequently, they receive more information and intelligence from their federal counterparts.

Moreover, many law enforcement agencies generate their own information and intelligence (much of which is collected in a sensitive manner) that is passed to other law enforcement agencies for their possible action. Law enforcement agencies have also begun to share information with new stakeholders in the fight against terrorism. They now routinely share information with non law enforcement government agencies and members of the private sector in order to assist in prevention efforts. This activity has altered the information sharing paradigm.

Another issue that exists within the current environment is the apparent "over classification" of material. Over-classifying data results in information and intelligence not being sent to the law enforcement professionals on the front lines of the fight against terrorism in this country the officers, troopers, and deputies in the field. It still appears to be a difficult process for the federal intelligence community to develop "tear-line" reports that can be passed to law enforcement so that the intelligence can be operationalized in an effective and proactive manner. Up until a short time ago, there was a lack of a coherent, standardized process for marking and handling SBU data. Lack of consistency in markings led to confusion and frustration among local, state, tribal, and federal government officials and also a lack of confidence in knowing that the information that was shared was handled in an appropriate and secure manner. Recent studies by the Government Accountability Office, the Congressional Research Service, and other institutions have confirmed and highlighted the problems created by the various markings and the lack of common definitions for these designations. These studies revealed that there are over 120 different designations being used to mark unclassified information so that agencies can "protect" their information. These pseudo classifications did not have any procedures in place outlining issues such as who can mark the material; the standards used to mark the material; who can receive the information; how the information should be shared, who it could be shared with, and how it should be stored; and what impact, if any, these markings have on the Freedom of Information Act.

As a result of several key federal terrorism related information sharing authorities, such as the Intelligence Reform and Terrorism Prevention Act of 2004, Executive Order 13388, and the December 2005 Memorandum from the President regarding Guidelines and Requirements in Support of the Information Sharing Environment, specifically Guideline 3, much work has been undertaken to bring about intelligence reform in this country. Local, state, and tribal law enforcement have been and continue to be active and collaborative participants in this undertaking.

As a representative of the New York State Intelligence Center (NYSIC)¹ and DOJ's Global Initiative, I have participated in a number of efforts to implement the guidelines and requirements that will support the ISE. Recognizing the need to develop a process for standardizing the SBU process, the CICC and GIWG commissioned a task team in May 2006 to develop recommendations that would aid local, state, and tribal law enforcement agencies in fully participating in the nationwide information sharing environment. This work was done with the Federal Bureau of Investigation, the U.S. Department of Homeland Security, the Office of the Program Manager for the Information Sharing Environment, and other law enforcement entities. The recommendations made by that team were provided to an interagency SBU working group. Subsequently, I participated on the SBU Coordinating Committee (CC) that was established to continue the Guideline 3 implementation efforts begun by the interagency group.

As you know, the SBU CC recommendations are currently under review and awaiting ultimate Presidential approval. The CC recommends adoption of a new Controlled Unclassified Information (CUI) Regime that is designed to standardize SBU procedures for information in the ISE. The recommendations include requiring controls on the handling and dissemination of SBU information. By and large, I believe local, state, and tribal agencies will support the new CUI Framework because they want to be active participants in the ISE and are supportive of clear and easily understandable protocols for sharing sensitive information.

Local, state, and tribal agencies want to be able to receive terrorism, homeland security, and law enforcement information from the federal government and clearly understand, based on the markings on the data, how the data should be handled and stored and to whom the information can be released. The data should be dis

¹Formerly known as the Upstate New York Regional Intelligence Center (UNYRIC).

seminated as broadly as possible to those with a need to know, including non law enforcement public safety partners, public health officials, and private sector entities. Conversely, local, state, and tribal entities are frequently the first to encounter terrorist threats and precursor criminal information, and the new CUI markings will assist with sharing that type of information both vertically and horizontally while respecting originator authority.

A number of critical issues must be addressed at the local, state, tribal and federal levels in order to facilitate a successful CUI Regime implementation, including training, policy and procedural changes, system modifications and enhancements, and funding to implement these recommendations.

Emphasis must be placed on the development and delivery of training to local, state, tribal, and federal personnel on the CUI Framework. Because of the possibility of wide distribution of sensitive information, it is imperative that training be given a priority so recipients have a clear understanding of marking and handling procedures. In order to maximize the effectiveness of the training and reach the appropriate recipients at the local, state, and tribal levels, I recommend that it be provided on a regional basis across the country to personnel in the designated state-wide fusion centers. Focusing on fusion center officials in the initial delivery phase directly supports the national information sharing framework that calls for the incorporation into the ISE of a national network of state and major urban area fusion centers.

In support of the ISE, state and major urban area fusion centers will be contributing information to ongoing federal and national level assessments of terrorist risks; completing statewide, regional, or site-specific and topical risk assessments; disseminating federally generated alerts, warnings, and notifications regarding time sensitive threats, situational awareness reports, and analytical products; and supporting efforts to gather, process, analyze, and disseminate locally generated information such as suspicious incident reports. Over 40 states currently have operational fusion centers, and it is critically important that center personnel receive timely, relevant training to enable them to fully function in the national ISE.

Training will provide insight and an understanding of how the CUI handling and disseminating requirements affect business processes. This will cause agencies to execute policy and procedural changes and system modifications. There are potentially over 18,000 local, state, and tribal law enforcement agencies in our country that could be impacted by the implementation of the CUI Framework. I believe that the federal government working collaboratively with local, state, and tribal authorities should develop model policies and standards to aid in the transition to the Framework. Funding issues will be a major factor for local agencies, especially in regard to modifying/enhancing information technologies and applying encryption requirements to ensure proper transmission, storage, and destruction of controlled information.

It will be through these ongoing collaborative efforts regarding Guideline 3 that the ISE will take another step towards being the meaningful and cooperative sharing environment that it was intended to be. These actions will result in the maturation of information sharing among state, local, and tribal agencies; private entities; and their federal counterparts, which will in turn assist in our collective efforts to prevent another terrorist attack and reduce violent crime. Our goal should be to share as a rule and withhold by exception, according to rules and policies that protect the privacy and civil rights of all.

Being involved in the CUI Framework development process has been a rewarding and sometimes arduous experience. It is a process that I and the entire state, local, and tribal law enforcement community take very seriously. It is very encouraging to me that the Office of the Program Manager and other relevant partner federal agencies have made great strides in recognizing the value that local, state, and tribal officials bring to the table. We want to remain active, ongoing partners and participants with the federal government as we work towards a national information sharing environment.

Mr. Chairman, I thank you and your colleagues for giving me the opportunity to speak to you today, and I hope my comments have been of some use to you in your deliberations.

Ms. HARMAN. But I would also note that our police, sheriffs and firefighters are our front lines. They take all the risks to keep our country safe, and on behalf of a grateful nation, we send, again, our condolences and appreciation to the New York State Police.

Today, we will also focus on how best to support the CUI framework at the federal level. That is why DHS and FBI are testifying.

Last month, we learned that every agency in the federal government has invented pseudo-classifications for their particular brand of information. The increasing number of these markings has led to tremendous confusion.

Obviously, that proliferation is a problem, and our goal here is to find out whether Ambassador McNamara's new framework is one that will be embraced, as it should be, by those federal agencies that are in the same line of work. If we can't get it right at the federal level, we can't expect state and local entities to do any better. We are late in this process, and we can and should move faster.

I hope this hearing will help us figure out how to move from a good proposal to a good adopted strategy across the federal government and with our state and local partners.

I would like to, again, extend a warm welcome to our witnesses who will be talking about these issues, and I look forward to your testimony.

I now yield time for opening remarks to the ranking member, Sheriff Reichert.

Mr. REICHERT. Thank you, Madam Chair. I like that "sheriff" title. Thank you for using that.

I, first of all, apologize. My voice is a little hoarse this morning. I am experiencing some effect from the oak pollen, I think, that is flying around out here. I am not used to that back in Seattle.

Second, let me also share my condolences with the New York State Police. I have experienced the loss of heartbreak myself in my 33-year career, and that is a tough one to take.

Also, Ambassador, I would like to thank you for your briefing earlier this week. It was very helpful, and thank you again for being here today to share your thoughts on your new ideas and plans.

I also want to say that I certainly recognize the difficulty that all three of you have in bringing the nation's state and local and federal agencies together to share information. Just on the local level, in the Seattle region, I know how tough that can be. So your job is going to be very tough, as we all recognize, but we certainly want to be a part of the solution with you.

So today we meet on a topic of pseudo-classification, which is the use of document controls that protect sensitive but unclassified information. This is the second hearing in a series on the problems of over-classification and pseudo-classification and information sharing.

I believe it is essential that sensitive information be able to flow to those that need it, and I shared a story the other day with the ambassador, my own personal experience within the sheriff's office, people holding and withholding information and other police departments not wanting to share the information and therefore resulting in maybe a case not being resolved or solved or being solved much later than it could have.

Information needs to flow in a trusted information sharing environment. The people who share sensitive information need to be able to trust that different federal agencies, as well as different states and localities, will treat their information with respect and protect sensitive information.

Currently, there is no trusted information sharing environment for sensitive, unclassified information. There are currently over 107 unique markings for sensitive information and over 130 different labeling or handling processes, as we talked about the other day. This disparity creates confusion and leads to information not being properly protected. If a federal agency can't trust that sensitive, unclassified information will be protected, it will simply classify the document as secret or above, severely restricting access.

If a private-sector entity or state/local agency does not believe its information will be protected properly, it simply will not share that, and I have experienced that myself. So without trust, the information sharing environment breaks down.

Creating a trusted environment is essential to the work of the program manager. Cleaning up a messy system of sensitive but unclassified designations is essential to creating that trust.

We are looking forward to the program manager's testimony as well as the testimony of our DHS and FBI witnesses who will be able to discuss how these policies are progressing and how we can ensure the information sharing is a success.

From the second panel, hopefully, we will hear from state law enforcement. We have had a role in the process. The state and local perspective is essential, because without the state and local buy-in, as I said, collaboration will lead to not sharing information.

We appreciate your testimony and your time this morning, and thank you again for being here.

With that, I yield the balance of my time.

Ms. HARMAN. The gentleman's time has expired.

The chair now recognizes the chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much, Madam Chair, and I join you in welcoming our distinguished witnesses today to this important hearing on the work being done by Ambassador McNamara.

I also join you and our ranking members and others in expressing our heartfelt sympathies to the New York State Police in the loss of their officer. Any front-line person puts his or her life on the line every day, and, unfortunately, sometimes these things happen. And that is why what we and is so important every day and what so many others do.

But from information sharing, I think Representative Reichert spoke volumes when he said it is important to have information available in real-time. I was in local government before coming to Congress and I remember when agencies bragged about knowing something, and when other folks found out about it weeks and months later, they would say, "Well, we knew about that all the time."

To me, it is a no-brainer not to share the information if we are supposedly all looking for the bad guys—or gals, in some instances.

Ms. HARMAN. You had it right the first time, Mr. Chairman.

[Laughter.]

Mr. THOMPSON. But the notion is we absolutely need to do it, but we are concerned that sometimes government over-classifies information so that it can't get out into the field.

And, Ambassador, I know you have a tough challenge ahead of you. We talked a little bit about it before the hearing, and I am looking for this new framework. I want the commitment to be there, to carry it forward. I would not like to see it become another in a long line of acronyms that get put on the shelf never to be taken off. So I look forward to your testimony, and I look forward to pushing forward the new ideas.

The comfort zone, as all of us know, is we have always done it this way, but that doesn't necessarily mean that it is correct. And these are different times, different challenges and it calls for broader strategies.

So I look forward to the testimony and the questions to follow. And I yield back.

Ms. HARMAN. The gentleman's time has expired.

And I would just observe, the comfort zone ended on 9/11. There is no comfort zone anymore. I am looking at a press clip today in the New York Times, which says, "British anti-terrorism chief warns of more severe al-Qa'ida attacks." These are in Britain, but obviously we can imagine this here.

So in that spirit, I would hope that what we are talking about never hits a shelf. That should not even be an option. We have to change the way we do business.

I welcome our first panel of witnesses.

Our first witness, Ambassador Ted McNamara, is the program manager of the Information Sharing Environment, a position established by the Intelligence Reform and Terrorism Prevention Act of 2004, a statute I am very familiar with.

Ambassador McNamara is a career diplomat who originally retired from government service in 1998, after which he spent 3 years as president and CEO of the Americas Society and Council of the Americas in New York. Following the September 11 attacks, he was asked to return to government service as the senior advisor for counterterrorism and homeland security at the Department of State.

Our second witness, Dr. Carter Morris, is currently director of information sharing and knowledge management for the Office of Intelligence and Analysis at the Department of Homeland Security. That is a mouthful. That can't even be one business card.

He is a detailee to DHS from the Directorate of Science and Technology at CIA. Most recently, Dr. Morris served as the deputy assistant director of Central Intelligence for Collection where he helped coordinate all intelligence community collection activities.

Thank you for that service.

Our third witness, Wayne Murphy, is currently an assistant director at the FBI. He joined the bureau with more than 22 years of service at the National Security Agency in a variety of analytic, staff and leadership positions. The bulk of his career assignments have involved direct responsibility for SIGINT analysis—that is signals intelligence analysis and reporting—encompassing a broad range of targets.

Without objection, the witnesses' full statements will be inserted in the record, and I would ask each witness to summarize your statements.

I think this time clock is visible to you, or I think it can be, or there is a time clock that is visible to you. And we will get right into questions following your testimony.

Thank you.

We recognize you first, Dr. Morris. Dr. Morris, we are recognizing you first. I am not sure why we are doing that, but that is what we are doing.

Mr. MORRIS. Didn't realize I was going to go first, but I will be very happy to do that.

Ms. HARMAN. Dr. Morris, you are relieved of going first.

[Laughter.]

Mr. MORRIS. Thank you.

Ms. HARMAN. Because this chair, who must be visually impaired, skipped the top of the statement.

Ambassador McNamara, you are recognized first. I think that does make more sense, because you are going to present the information, and then we will follow on with two people who will comment on it, which seems obvious. I apologize for the confusion.

**STATEMENT OF AMBASSADOR THOMAS E. McNAMARA,
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT,
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

Mr. McNAMARA. Thank you very much, Madam Chair.

Chairman Thompson, Madam Chairman Harman, Ranking Member Reichert and members of the subcommittee, it is a great pleasure to be here with my colleagues today. And I want to thank you for the continued focus and priority for building an effective information sharing environment that you and the committee have shown over the course of many months.

I hope to especially discuss with you all work on the presidential priority to standardized sensitive but unclassified information.

Our current efforts to provide the president recommendations for standardizing SBU procedures, sensitive but unclassified, have been successful because of the strong interagency commitment that we have found. I want to note that Wayne Murphy, who is a member of the SBU Coordinating Committee with me, has been a part of this process since the very beginning and, with his colleagues in the Department of Justice and the FBI, have been instrumental in bringing the state, local and private sector perspectives and concerns to the table.

I also was hoping to thank Colonel Bart Johnson were he here today, but I will thank him in his absence. He is the chair of the Criminal Intelligence Coordinating Council of Global Justice Information Sharing Initiative. He has been giving so much of his time and expert advice to our group, and I join the committee in offering our condolences to the family of the slain officer and to Colonel Johnson and his colleagues.

I have a personal sense of this loss. My son is a law enforcement officer and has been in a situation that occurred in the last 24 hours himself.

Also, I would like to thank assistant commissioner for the Florida Department of Law Enforcement, Mark Zadra, who is here today, who was our host at the very first national conference on fu-

sion centers, which was held earlier this year in Florida. It was an excellent, very astonishing, in some respects, conference. Over 600 people came to that conference. They closed the rolls for the conference about 3 or 4 weeks before the conference began.

When I showed up in this job a year ago, if someone had told me in a year that that would happen, I would have said, "Well, you people are just overly optimistic." And I think that shows how far things have gone over the course of the last few years.

Finally, I want to note that the Department of Justice and Department of Homeland Security were leaders in the initial effort to research this issue on SBU and to collect the information on which my committee has been working these last 6 months.

The lack of government-wide standards for SBU information is well known. More difficult has been charting a feasible way ahead to create such standards as part of a single regime. Over the years, because SBU is not considered a matter of national security concern, there has been no single control framework that enables the rapid and routine flow of this type of information.

Throughout the Cold War, executive branch agencies and Congress responded in a piecemeal fashion, an uncoordinated way, to protecting SBU. It was left to each agency to decide on its control regime.

For example, there are close to 107 unique markings and more than 131 different labeling or handling processes and procedures for SBU information. These markings and handling processes stem from about 280 statutory provisions and approximately 150 regulations.

Protecting information and sharing information are critical and interdependent functions for the information sharing environment. Simply stated, sensitive information will not be shared unless participants have confidence in the framework protecting that information.

Standardizing SBU procedures is a difficult endeavor made more complicated by the complex information management policies and practices which the government now has. Correcting these defects is especially important because some categories of SBU truly require controls as strong as those for national security information.

There are sound reasons in law and policy to protect those categories from public release, both to safeguard the civil liberties and legal rights of U.S. citizens and to deny the information advantage to those who would threaten the security or the public order of the nation.

Appropriately protecting law enforcement and homeland security related sources and methods, for example, are just as valuable to our nation as protecting our intelligence sources and methods. The global nature of the threat our nation faces today requires that our entire network of defenders be able to share information more rapidly and confidently so that those who must act have the information they need to act.

This lack of a single rational standardized and simplified SBU framework is a major cause of improper handling. It heightens risk aversion and undermines the confidence in control mechanisms. These problems are endemic within the federal government between federal and non-federal agencies and with the private sector.

This is a national concern because the terrorist threat to the nation requires that many communities of interest, at different levels of government, share information.

Ms. HARMAN. Ambassador McNamara, let me suggest that you just describe the new system, and we can get into the arguments for it and so forth in the question period, because your 5 minutes has expired.

Mr. McNAMARA. Okay. I will then move to saying that I think this new system will enhance our ability to share vital information at the state, federal, local, tribal and private sector entities and also with our foreign partners.

There are three major elements to the standardized SBU system that I am proposing. First, is the CU designation. The committee has decided that a clean break with the current SBU system would begin by calling it, controlled, unclassified information, CUI, thus eliminating the old term of SBU and any residual or legacy controls and habits that have grown up.

Secondly, CUI markings, there will be a CUI framework recommended that also contains mandatory policy and standards for making safeguarding and dissemination of all CUI originated at the federal government level and shared in the ISE regardless of the medium used for its display, storage or transmittal. This framework includes a very limited marking schema that addresses both safeguarding and dissemination.

Thirdly, there will be CUI governance recommended. A central management and oversight authority in the form of an executive agent and an advisory council would govern the new CUI framework and oversee its implementation. This CUI framework is one of the essential elements among many elements that make up the ISE.

And since my time is short and over, I guess, I will say that I would like to close by saying how helpful and important it is to the work that I am doing for the Congress to focus on this matter, as this committee and subcommittee has done. This is a high-priority matter creating the ISE and in particular it is important that the amount and quality of the collaboration on implementing these reforms be noted and enhanced so that we can strengthen our counterterrorism mission at all levels of government.

Thank you.

[The statement of Mr. McNamara follows:]

PREPARED STATEMENT OF ABASSADOR THOMAS E. MCNAMARA

I. Introduction

Chairwoman Harman, Ranking Member Reichert, and Members of the subcommittee: I am pleased to be here with my colleagues and want to thank you for your continued focus and priority to building an effective Information Sharing Environment (ISE).

As you and the Committee address classification of information issues, I would like to update you on a Presidential priority to standardize procedures for Sensitive But Unclassified (SBU) information. This is a priority because if we do not have a manageable SBU framework, we will not have an effective ISE.

Information vital to success in our protracted conflict with terrorism does not come marked "terrorism information"; it can and does come from many sources, including from unclassified information sources. Yet we lack a national unclassified control framework that enables the rapid and routine flow of information across

Federal agencies and to and from our partners in the State, local, tribal and private sectors. This is especially important because some categories of unclassified information require controls as strong as those for national security information. There are sound reasons to protect those categories from public release, both to safeguard the civil liberties and legal rights of U.S. citizens, and to deny the information advantage to those who threaten the security or public order of the nation.

This lack of a single, rational, standardized, and simplified SBU framework is a major cause of improper handling. It heightens risk aversion and undermines confidence in the control mechanisms. This leads to both improper handling and unwillingness to share information. These problems are endemic within the Federal government, between Federal and non Federal agencies and with the private sector. This is a national concern because the terrorist threat to the nation requires that many communities of interest, at different levels of government, share information. They must share because they have each have important responsibilities in countering terrorism. The problem exists at all levels—Federal, State, local, tribal, and the private sector. All have cultures that are traditionally cautious to sharing their sensitive information, but this must be addressed if we are to properly and effectively share sensitive but unclassified information. Only when the Federal government provides credible assurance that it can protect sensitive data from unauthorized disclosure through standardized safeguards and dissemination controls will we instill confidence that sensitive information will be appropriately shared, handled, safeguarded, and protected, and thus make sharing part of the culture.

II. The Current SBU Environment

Let me note at the outset that I will focus here on “unclassified” information. Classified information is, by law and regulation, controlled separately in a single system that was established early in the Cold War years. The classification regime, currently governed by Executive Order 12958, as amended, applies to “national security information,” which includes intelligence, defense, and foreign policy information. Other information, which legitimately needs to be controlled, is controlled by agency specific regimes. Collectively, these regimes address information referred to as Sensitive But Unclassified (SBU) information. SBU information has grown haphazardly over the decades in response to real security requirements, but this information cannot be encompassed in the subject specific classified control regime. The result is a collection of control mechanisms, in which most participants have confidence only when information is shared within an agency and sometimes not even then.

Let me give you some understanding of how complex SBU is: Among the 20 departments and agencies we have surveyed, there are at least 107 unique markings and more than 131 different labeling or handling processes and procedures for SBU information. Even when SBU information carries the same label marking (e.g. For Official Use Only), storage and dissemination are inconsistent across Federal agencies and departments. Because such markings are agency specific, recipients of SBU information in a different agency must understand the processes and procedures of the originating Federal agency for handling the information, even if their agency uses the same marking. The result is an unmanageable collection of policies that leave both the producers and users of SBU information unable to know how a piece of information will be controlled as it moves through the Federal government and therefore reducing information sharing.

I would like to highlight just two examples to convey the confusion created by the current SBU processes:

The first example is a single marking that is applied to different types of information. Four agencies (DHS, DOT, USDA and EPA) use “SSI” to mean “Sensitive Security Information.” However, EPA has also reported the use of “SSI” to mean “Source Selection Information” (i.e. acquisition data). These types of information are completely different and have vastly different safeguarding and dissemination requirements, but still carry the same SBU marking acronym. In the same way, HHS and DOE use “ECI” to designate “Export Controlled Information,” while the EPA uses “ECI” to mean “Enforcement Confidential Information.” “Export Controlled Information” and “Enforcement Confidential Information” are clearly not related, and in each case, very different safeguarding and dissemination controls are applied to the information. The second example is of a single marking for the same information, but with no uniformity in control. Ten agencies use the marking “LES” or “Law Enforcement Sensitive.” However, the term is not formally defined by most agencies nor are there any common rules to determine who can have access to “law enforcement information.” Therefore, each agency decides by itself to whom it will disseminate such information. Thus, an individual can have access to the information in one agency but be denied access to the same information in another. Further con

fusing the situation, SBU markings do not usually indicate the originating entity. As a result, even if a recipient had access to all the different control policies for each agency, he or she could probably not determine what rules apply because the recipient usually does not know which agency marked the document.

Protecting the sharing of information is a critical and interdependent function for the ISE. Simply stated, sensitive information will not be shared unless participants have confidence in the framework controlling the information. Standardizing SBU procedures is a difficult endeavor, made more complicated by the complex information management policies.

III. Unclassified Information Framework Imperative

Producers and holders of unclassified information which legitimately needs to be controlled must have a common framework for protecting the rights of all Americans. In the classified arena, we deal with information that will, mainly, be withheld from broad release. In the unclassified arena, we deal with information that is mainly shareable, except where statute and policy require restrictions. Agencies must often balance the need to share sensitive information, including terrorism-related information, with the need to protect it from widespread access.

A new approach is required. Existing practices and conventions have resulted in a body of policies that confuse both the producers and users of information, ultimately impeding the proper flow of information. Moreover, multiple practices and policies continue to be developed absent national standards. This lack of standards often results in information being shared inappropriately or not shared when it should be. In December 2005, the National Industrial Security Program Policy Advisory Committee, described the consequences of continuing these practices without national standards in the following manner ". . . the rapid growth, proliferation and inclusion of SBU into classified contract requirements without set national standards have resulted in pseudo security programs that do not produce any meaningful benefit to the nation as a whole." Clearly this situation is unacceptable.

IV. A Presidential Priority

The lack of government wide standards for SBU information is well known. More difficult has been charting a reasonable way ahead to create such standards. This is an enormously complex task that requires a careful balance between upholding the statutory responsibilities and authorities of individual departments and agencies, and facilitating the flow of information among them all the while protecting privacy and civil rights. We were successful in creating such a regime for classified national security information by setting national standards and requiring that they be executed uniformly across the Federal government. In addition, we established a permanent governance structure for managing the classified information regime. A similar approach is necessary to establish an unclassified information regime, with standards governing controlled unclassified information.

As required by the Intelligence Reform and Terrorism Prevention Act of 2004, on December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*, which specified tasks, deadlines, and assignments necessary to further the ISE's development. Guideline 3, of his Memorandum, specifically instructed that to promote the sharing of, ". . . Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information,¹ procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State; local, and tribal governments, law enforcement agencies, and private sector entities."

An interagency SBU Working Group, co chaired by the Departments of Homeland Security (DHS) and Justice (DOJ), undertook an intensive study and developed several draft recommendations for a standardized approach to the management of SBU. Its work provided a solid foundation for completing the recommendations. It was de-

¹ Pursuant to the ISE Implementation Plan, and consistent with Presidential Guidelines 2 and 3, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.

terminated, however, that additional work was necessary to fully meet the requirements of Guideline 3.

Recommendations for Presidential Guideline 3 are coming close to completion in a SBU Coordination Committee (SBU CC), chaired by the Program Manager, Information Sharing Environment (PM ISE), with Homeland Security Council oversight. The SBU CC began work in October 2006 with the participation of the Departments of State, Defense, Transportation, Energy, Justice, and Homeland Security; the Federal Bureau of Investigation; the Office of the Director of National Intelligence; the National Security Council; and the Office of Management and Budget. The committee actively consults with representatives from other departments and agencies, the National Archives and Records Administration (NARA), the Information Security Oversight Office, the Controlled Access Program Coordination Office, the Information Sharing Council, the Global Justice Information Sharing Initiative, State, local, and tribal partners, and several private sector groups.

The efforts of the SBU CC have focused on developing an SBU control framework that is rational, standardized, and simplified, and as such, facilitates the creation of an ISE that supports the individual missions of departments and agencies and enhances our ability to share vital terrorism information among Federal, State, local, tribal, and private sector entities, and foreign partners.

- **RATIONALIZATION** means establishing a framework based on a set of principles and procedures that are easily understood by all users. This should help build confidence among users and the American public that information is being shared and protected in a way that properly controls information that should be controlled, and protects the privacy and other legal rights of Americans.

- **RATIONALIZATION** means structuring a framework in which all participants are governed by the same definitions and procedures and that these are uniformly applied by all users. The objective is to end uncertainty and confusion about how others using the framework will handle and disseminate SBU information. Standardization helps achieve the ISE mandated by Congress: "a trusted partnership between all levels of government."

- **SIMPLIFICATION** means operating a framework that has adequate, but carefully limited, numbers and types of markings, safeguards, and dissemination of SBU information. Such a simplified framework should facilitate Federal, State, and local government sharing across jurisdictions; facilitate training users; and reduce mistakes and confusion.

V. The Controlled Unclassified Information (CUI) Framework

I must reiterate that interagency discussions of a proposed detailed framework are still underway. Furthermore, no recommendation will become final unless and until it is approved by the President. Of course, the ability to implement any reform will depend upon the availability of appropriations. With respect to the present proposal, however there is general agreement that the SBU framework should include the following 6 main elements:

1. **CUI DESIGNATION:** To ensure a clean break with past practices, the Framework would change the descriptor for this information to "Controlled Unclassified Information" (CUI) thus eliminating the old term "SBU." Participants would use only approved, published markings and controls, and these would be mandatory for all CUI information. All other markings and controls would be phased out.

2. **CUI MARKINGS:** The CUI Framework also contains mandatory policies and standards for marking, safeguarding and dissemination of all CUI originated by the Federal government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal. This Framework includes a very limited marking schema that addresses both safeguarding and dissemination. It also provides reasonable safeguarding measures for all CUI, with the purpose of reducing the risk of unauthorized or inadvertent disclosure and dissemination levels that with the purpose of facilitating the sharing of CUI for the execution of a lawful Federal mission or purpose.

3. **CUI EXECUTIVE AGENT:** A central management and oversight authority in the form of an Executive Agent would govern the new CUI Framework and oversee its implementation.

4. **CUI COUNCIL:** Federal departments and agencies would advise the Executive Agent through a CUI Council composed of senior agency officials. The Council will also create mechanisms to solicit State, local, tribal, and private-sector partner input.

5. **ROLE OF DEPARTMENTS AND AGENCIES:** The head of each participating Federal department and agency will be responsible for the implementation of a functional CUI Framework within the agency.

6. **CUI TRANSITION STRATEGY** a Transition Strategy for a phased transition from the current SBU environment to the new CUI Framework is needed. During the transition, special attention would be paid to initial governance, performance measurements, training, and outreach components.

On a final note, our work has recognized that the substantive information that will be marked and disseminated in accordance with the proposed Framework is also subject to a variety of other legal requirements and statutes. Among some of

the most important statutes and legal authorities that apply to this information are the Privacy Act of 1974, the Freedom of Information Act, the Federal Information Security Management Act (FISMA) and various Executive Orders, including Executive Order 12333, which governs the Intelligence Community and its use of United States Persons information. I would like to stress that this proposed Framework for handling SBU has thoroughly considered these legal authorities and does not alter the requirements and obligations imposed by these authorities. We will continue to work with the ISE Privacy Guidelines Committee to ensure that the appropriate privacy issues fully meet any legal requirements to protect the civil liberties and privacy of Americans.

VI. Conclusion

For information sharing to succeed, there must be trust the trust of government providers and users of information, or policymakers, and most importantly, of the public. Each of these must trust that information is being shared appropriately, consistent with law, and in a manner protective of privacy civil liberties. Building trust requires strong leadership, clear laws and guidelines, and advanced technologies to ensure that information sharing serves important purposes and operates consistently with American values.²

The lack of a single, rationalized, standardized, and simplified SBU framework does contribute to improper handling or over-classification. To instill confidence and trust that sensitive information can be appropriately shared, handled, safeguarded, and protected, we must adopt a standardized CUI Framework. This is especially critical to our counterterrorism partners outside the intelligence community. Appropriately protecting law enforcement and homeland security related sources and methods are just as valuable to our national security as protecting our intelligence sources and methods.

The global nature of the threats our Nation faces today requires that: (1) our Nation's entire network of defenders be able to share information more rapidly and confidently so that those who must act have the information they need, and (2) the government can protect sensitive information and the information privacy rights and other legal rights of Americans. The lack of a government-wide control framework for SBU information severely impedes these dual imperatives. The CUI Framework is essential for the creation of an ISE which has been mandated by the President and the Congress. Only then can we meet the dual objectives of enabling our Nation's defenders to share information effectively, while also protecting the information that must be protected. A commitment to achieving standardization is essential a vital need in the post 9/11 world.

Ms. HARMAN. Thank you, Ambassador.

We now recognize Dr. Morris for a 5-minute summary.

STATEMENT OF CARTER MORRIS, Ph.D., DIRECTOR, INFORMATION SHARING AND KNOWLEDGE MANAGEMENT, OFFICE OF INTELLIGENCE AND ANALYSIS, DHS

Mr. MORRIS. Thank you, Madam Chairman, Chairman Thompson, Ranking Member Reichert, other distinguished members of the subcommittee.

It really is a pleasure for me to be here this morning to talk about the activities that we are doing in DHS relative to information sharing and specifically to talk about the activities that we are doing with Ambassador McNamara, the FBI, our other federal partners and our state and local partners in developing a system that will effectively allow us to share information but also to protect the information that needs to be protected.

When I go around and give my various talks that I give on information sharing, I like to quote from the Homeland Security Act that says one of the responsibilities of DHS is to share relevant and appropriate homeland security information with other federal agencies and appropriate state and local personnel together with

²*Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, Third Report of the Markle Foundation Task Force, July 2006

assessments of the credibility of such information. And the act defines state and local to include the private sector.

I think that is my charge in DHS to make that happen and that we take that very seriously that that is a major part of the responsibilities of the Department of Homeland Security.

The challenge that we face, and the one we are talking about here today, is the issue that being able to share but to still protect the information that needs to be protected. Now, I know from the Congress we hear both things coming at us strongly, and we want to make sure that we do both effectively.

In the national security community, we have had a classification system in place for a very long time. You can argue as to what is in it and what is out of it, but let me assure you, even in that community, we continue to look at need to know and originator control and third agency rules, all the things that people believe are an impediment to sharing, all of which are actively being debated at the moment.

Outside of the national security community, as we have already talked about, there are also reasons to protect information. Some of this information is very vital to national security—privacy, law enforcement case information, witness protections, security practices, vulnerabilities in our critical sectors and even lots of others.

These are very legitimate reasons, and what we have to do is figure out how to share, how to protect and how to build trust in the system, as Ranking Member Reichert pointed out, so that people will actually share the information. And that is the challenge that we have.

Let me add a little bit of my own personal assessment here, speaking for myself. As I look around the information sharing business, information that is what I would call important is rarely not protected in some way. So in almost everything we talk about in information sharing, we have to couple that with a discussion of information protection. And so we can't talk about one without the other.

We believe that DHS has moved forward in the information sharing business. If you look at my written statement, you will see that there are a number of references made, the things we have done. I would like to point out just two, and one of them is very relevant today.

One is, in the classified domain, we have led a community effort with all of our partners to look at how we better produce unclassified tear lines from classified reporting and to not only produce that tear line with information but produce an assessment, let me say, of the credibility of that information. We believe we have a new system that is currently being implemented, and some of my intelligence community partners we have already seen a real change in how that is being implemented.

The second area on the non-classified side is all of the efforts that we have put into working the controlled, unclassified information. As Ambassador McNamara said, DHS, working with the Department of Justice, that really started that planning into these activities, and we take this as a very important thing to accomplish. Some of the people who work for me are very rabid about the issue that we really do need to get this under control and do it very well.

So that is the area that we really need to work on, this regime for how we handle and control information.

Let me say that when we do this regime of looking at how this controlled, unclassified information, we believe there are three things that we particularly need to pay attention to. One is that we put in place a governance structure to run this, and we put it in quickly, effectively and from the beginning.

The second thing is we believe any system is going to have to be easy to use. It is going to have to be convenient.

And the third thing is that we believe that we are going to have to make sure that any system that we put in at the federal level is closely coordinated with the state and locals and how they handle information. As we know, there is law enforcement information at the federal level, there is law enforcement information at the state level. They are controlled differently, and we need to bring those systems together.

Let me finish up then, since my light is on, and very quickly. One, we are dedicated to information sharing. We are dedicated to implementing a new system to run the controlled, unclassified information. We are very much on board with the program and the proposal that is currently being proposed.

However, I will say, I do not believe this is easy. It is not easy at all, and I think that we are going to have to pay particular attention. We believe the phased approach that is in the initial proposal and how to get into this, we believe, is the right proposal.

And I am here now to answer any questions that you might like to ask.

[The statement of Mr. Morris follows:]

PREPARED STATEMENT OF DR. CARTER MORRIS

APRIL 26, 2007

Good morning, Chairwoman Harman, Ranking Member Reichert, and distinguished members of the subcommittee. My name is Carter Morris, and I am the Director of Information Sharing and Knowledge Management for the Office of Intelligence and Analysis at the Department of Homeland Security (DHS). It is a pleasure to be with you today to discuss the control of government information and the actions DHS is taking to address and improve our ability to share information without unnecessary restrictions and in a manner that protects what needs to be protected.

The Homeland Security Act of 2002 authorizes DHS to access, from any agency of the Federal government, state, local, and tribal governments, and the private sector, all information relating to threats of terrorism against the United States and other areas; information relating to the vulnerabilities of the United States to terrorism; and information concerning the other responsibilities of the Department as assigned to and by the Secretary. After analyzing, assessing, and integrating that information with other information available to DHS, the Secretary must then ensure that this information is shared with state, local, and tribal governments; and the private sector, as appropriate. Concomitant with these responsibilities is the obligation of the Secretary to identify and safeguard all homeland security information that is sensitive, but unclassified, and to ensure its security and confidentiality. Information sharing, for counterterrorism and related purposes, therefore, is key to the mission of DHS.

Moreover, the Intelligence Reform and Terrorism Prevention Act of 2004 established the Program Manager of the Information Sharing Environment (PM ISE) to assist in the development of policies, procedures, guidelines, rules, and standards, including those which apply to the designation, marking, and handling of sensitive but unclassified information, to foster the development and proper operation of the ISE. DHS, in coordination with the PM ISE and other agencies on the Information Sharing Council, is actively participating in efforts to standardize procedures for

sensitive but unclassified information and create an effective Information Sharing Environment.

The Challenge

The challenge that we face in handling information is balancing two important and competing factors: "sharing the information that needs to be shared" and "protecting information that needs to be protected." Our goal is to share information unless there is a valid and necessary reason to protect such information and thus limit or control the dissemination to a discrete community or other set of users.

The legitimate need to *classify* some information, for purposes of national security and to protect our sources and methods and allow information collection operations to be conducted without advanced notice to our adversaries, is well established. As sources and methods for acquiring information change, as well as our adversaries capabilities, we continue to evaluate and adjust our classification criteria.

Similarly, there are many indisputably legitimate reasons for protecting certain unclassified information, which we refer to generically as Controlled Unclassified Information (CUI)—for example, privacy concerns relating to personal information, the danger of compromising ongoing law enforcement investigations or of endangering witnesses, the need to protect private sector proprietary information and, most importantly, the need to protect information containing private sector vulnerabilities and other security-related information that could be exploited by terrorists. Unauthorized disclosure of this information could cause injury to a significant number of individual, business, or government interests.

Through DHS's work with state and local fusion centers, we have encountered examples of how the proliferation of internal policies for handling unclassified but sensitive information can create unintended barriers to information sharing. Existing markings that are meant to identify necessary safeguards and dissemination restrictions on information often create as much confusion as help. For example, a state fusion center received a report that contained actionable threat information bearing the marking "LES", meaning Law Enforcement Sensitive. The fusion center personnel were unsure to what extent they could disseminate information with such a marking. When they contacted the originating Federal agency, they were unable to speak with someone who knew the data and could explain the disclosure rules. The fusion center personnel erred on the side of caution and did not share the information in this case not the best solution.

Sensitive information (classified or unclassified) is only shared by people who trust the systems, policies, and procedures that guide that sharing. Any lack of confidence regarding the operation and effectiveness of a system reduces the willingness of consumers to share the information, therefore limiting any benefits it might offer.

With that in mind, we continue working to transition from a historically risk averse approach to sensitive information sharing, to one where the risks are considered and managed accordingly, but consistent with a responsibility to provide information to our partners and customers who need it.

In order to implement the mandates of the Information Sharing Environment we must both produce material at the lowest sensitivity level appropriate to allow it to be easily shared with all who need it and ensure that processes for protecting information that needs to be protected are defined and effective.

DHS is leading information sharing

DHS has been a leader in establishing new approaches to information sharing—including federal sharing at all classification levels; sharing with our state, local, tribal, and territorial partners; and sharing with the private sector. In this sharing it is critical to address both operational needs and the appropriate security in transferring the information. I would like to talk about five specific DHS information sharing initiatives where we are addressing the need to share but still providing an appropriate level of control of this information.

1. Like other Federal departments and agencies, DHS shares information with state, local, and tribal partners through state and local fusion centers. We are providing people and tools to these fusion centers to create a web of interconnected information nodes across the country that facilitates the sharing of information to support multiple homeland security missions. Working with the Federal government and its partners to establish this sharing environment, DHS is ensuring that its processes and systems not only achieve the sharing necessary but also provide the protection and control of the information that gives all parties confidence and trust that the information is appropriately used and that information which needs to be protected such as personally identifiable information is appropriately controlled and protected.

2. DHS, DOJ and other federal entities are also creating a collaborative, unclassified information sharing community, based on establishing a trusted partnership between the fusion centers and the federal government. This environment is requirements driven, and focused on providing information to support the mission of the intelligence analysts, allowing both information sharing and collaboration with the state and local intelligence communities to encourage the development of mature intelligence fusion capabilities. A key to the development of such a sharing environment is providing a system and processes that build confidence that information will not only be shared but also protected and controlled as needed, which is what we are doing.

3. As part of the Presidential Guideline effort, DHS led an interagency working group that developed the "Recommended Guidelines for Disseminating Unevaluated Domestic Threat Tearline Reporting at the Unclassified Level." Federal agencies disseminate unclassified extracts from unevaluated classified threat reports to facilitate sharing of threat information with those on the domestic front lines. Federal dissemination of raw threat reporting to State and local authorities before the relevant Federal agencies can assess the specific threat has, at times, led State and Local authorities to misinterpret the credibility of the threat. This effort provided recommendations to support timely sharing of terrorist threat data with state and local officials with increased clarity on the credibility of the information while maintaining the appropriate security for sources and methods. These recommendations are now being implemented in the intelligence community.

4. DHS is also leading the Federal Coordinating Group, to create coordinated federal intelligence products at the lowest appropriate levels of classification, for dissemination to state, local, tribal and private sector communities. The Group will coordinate three categories of "federally coordinated terrorism information products"—time-sensitive threat/incident reporting, situational awareness reporting, and strategic or foundational assessments. For each category of products, the Group will ensure originating agencies validate sourcing, ensure substantive completeness, and tailor the analysis for state, local, tribal, and private sector use. The Group will coordinate the downgrading and/or "tearlining" of classified materials where appropriate levels of classification or control that permit wider state, local, tribal, and private sector use but do not jeopardize national security or other sensitivities. Again the key is providing the necessary information while also providing clear understanding of the necessary protection and control of this information.

5. And finally, DHS is active in the interagency group working to minimize the number of different CUI safeguard and dissemination requirements. We undertake these efforts with an eye toward facilitating appropriate information sharing and significant progress can be made by eliminating internal safeguarding and dissemination policies that are inconsistent throughout Executive agencies and that are occasionally overly protective of information. We are committed to developing a system for Controlled Unclassified Information that effectively facilitates sharing while at the same time protecting sensitive information that requires robust protection.

DHS Key CUI elements

There are three issues that we believe are critical to success in instituting an effective CUI framework.

First, an effective and continuing CUI governance structure must be established. The lack of a government wide governance structure is one of the primary reasons that we have been struggling to overcome confusion in this area. To advance the government's information sharing demands with the attendant need to appropriately safeguard sensitive information requires a permanent governance structure to oversee the administration, training, and management of a standardized CUI system.

Second, DHS believes that the improved CUI framework must be clear and easy to implement for all stakeholders. It is important that we can justify and defend all information that is so controlled. If the framework is not readily understood it will not be used. Furthermore, adoption must be swift. Establishing the governance structure will aid this process by documenting the rules and standardizing the policies, processes, and procedures for handling CUI across the federal government.

And third, we must ensure that all potential users of CUI have a clear understanding of the CUI framework so that we can facilitate a more effective and interactive information exchange. We understand that they have their own constraints surrounding systems and sensitive data, so we must work to identify mechanisms to integrate state and local systems with the Federal framework.

Addressing these elements will help provide transparency and build confidence to increase sharing across communities from intelligence to law enforcement, from law enforcement to the first responders, etc.

Challenges Facing CUI standardization

Over 100 CUI designators or markings have been identified, and each of these has arisen to address a valid need to protect information. Most are codified as internal policies and procedures, some of which have actually served to enhance information sharing, i.e., clearly defined control systems create a trusted environment that encourages information sharing. Less often, such designators or markings are the result of legislative and/or regulatory requirements to protect certain information in a particular way. These practices worked well within a local environment, but the challenge is to leverage the successful practices and build a trusted environment that bridges communities and domains. We must exercise caution, however, as we go forward to consider and, where appropriate, revise operational practices in a manner that can achieve both sharing and protection in an expanded community.

This caution is especially true in cases where controls were created more to facilitate, rather than limit, information sharing. Within DHS, there are three such information protection regimes—"Protected Critical Infrastructure Information (PCII)," "Sensitive Security Information (SSI)," and the newly established "Chemical Vulnerability Information (CVI)." Congress mandated these categories of information be protected and DHS promulgated regulations implementing these regimes. Each was specifically created to foster private sector confidence to increase their willingness to share with the federal government crucial homeland security related information. To date, PCII and SSI have been successful in this regard and have been well-received by the private sector. Moreover, these designations are ready examples of how robust control of information can actually promote appropriate sharing.

Summary

Because we are changing established cultures and procedures and moving forward, in coordination with the PM ISE, with a new framework for CUI, it is important that we adequately address all elements of its implementation. Governance, training, strategic communications, information technology systems planning, and the development of new standards and procedures are all important to the effective implementation of these reforms. Phased implementation and continuous incorporation of the lessons learned in this process are basic tenets of change management. It is important that the appropriate governance model is adopted to ensure systematic implementation of the framework and foster information sharing.

That said, DHS is fully committed to this new framework and is, moreover, pleased that the framework fully recognizes the difficulties of implementation by proposing, among other things, a planning phase and phased implementation. Doing so will allow a smoother implementation and reduce the risk of losing the confidence that non-federal partners have now found in current DHS programs.

DHS looks forward to continue working with the PM ISE, the Information Sharing Council, and each of our Federal partners, to address the challenges of what many perceive to be the "over-classification" of information. We believe we made great strides in identifying the challenges. We also believe the paths forward are paved for interagency success in improving the sharing of information and providing an appropriate and streamlined system for controlling sensitive information. Nevertheless, and notwithstanding the good progress we have made to date, we should not underestimate the challenges that exist for implementing a new system for standardizing and handling Controlled Unclassified Information across the Federal government.

Thank you for your time. I would be glad to answer any questions.

Ms. HARMAN. Thank you, Dr. Morris.

The chair now recognizes Mr. Murphy for a 5-minute summary of his testimony.

**STATEMENT OF WAYNE M. MURPHY, ASSISTANT DIRECTOR,
DIRECTORATE OF INTELLIGENCE, FEDERAL BUREAU OF
INVESTIGATION**

Mr. MURPHY. Good morning. Thank you, Madam Chairman Harman, Chairman Thompson, Ranking Member Reichert and members of the subcommittee.

I am pleased to be here today to demonstrate the commitment of the Federal Bureau of Investigation to strengthening our nation's ability to share terrorism information. We are diligently

working to fulfill the expectations that Congress set forth in the Intelligence Reform and Terrorism Prevention Act of 2004.

As the assistant director for intelligence to the FBI and the FBI's senior executive for information sharing, I am at once responsible for, accountable to, and have a vested interest in a successful information sharing environment.

I am particularly pleased to be testifying today with Ambassador Ted McNamara and Dr. Carter Morris. It has been my privilege over the past many months to work with these professionals and many others as we seek to craft an outcome that matches both the letter and spirit of the task before us.

I join them today to discuss our collective efforts to develop a standardized framework for marking, safeguarding and sharing controlled, unclassified information. My nearly 24 years in the intelligence community have largely been served in an environment where I dealt almost exclusively with classified national security information.

While those regimes could be complicated and require great discipline and attention to detail, by comparison, they are far less challenging than my experience has been in working to organize a functional CUI framework. This is not because of a lack of commitment, focus and creativity and trying to address that framework but because of the myriad of issues and interests that one encounters in the transitional world of information between what is controlled and what is not.

From an FBI perspective, getting it right is especially important. Our information sharing environment spans the range from classified national security information to fully open source. We must have the capacity to interpose information from all of these regimes and to do so in a dynamic manner. We must have the agility to rapidly move information across security barriers and into environments that make it more readily available and therefore of greater value to the broadest set of players.

And across all of our partners, we must have a framework that allows for an immediate and common understanding of information's provenance and the implications that that imparts. We must make the sharing of CUI a benefit, not a burden, especially on state, local and tribal police departments who would be disproportionately affected if asked to sustain a complex and expensive control framework. We must manage information in way that sustains the confidence of people and organizations who share information that puts them and their activities at risk.

Most important of all, we must respect the power of that information and the impact it holds for the rights and civil liberties of American people who have trusted us to be its stewards. That means we must also never use control as a way to deny the public access to information to which they are properly entitled.

With the FBI, achieving a streamlined CUI framework is much more than establishing a process; it is about shaping mindsets so that we can shift fully from a need to know to a duty to provide. The CUI framework, as proposed, creates opportunities and solves problems for me that I could not have solved on my own. The FBI is fully and completely committed to this process.

All of us who have been part of this process wish we could move more quickly in reaching a point where we are today, but I believe the investment of time, the level of effort and the openness and commitment that has marked our dialogue has done justice to the expectations of the American people.

Thank you for this hearing. I look forward to answering your questions.

[The statement of Mr. Murphy follows:]

PREPARED STATEMENT OF WAYNE M. MURPHY

APRIL 26, 2007

Good morning, Chairman Harman, Ranking Member Reichert, and members of the Subcommittee. I am pleased to be here today to demonstrate the commitment of the Federal Bureau of Investigation (FBI) to strengthening our nation's ability to share terrorism information. We are diligently working to fulfill the expectations Congress set forth in the Intelligence Reform and Terrorism Prevention Act of 2004. As the Assistant Director for Intelligence and the FBI Senior Executive for Information Sharing, I am at once responsible for, accountable to and have a vested interest in a successful Information Sharing Environment.

I am particularly pleased to be testifying today with Ambassador Ted McNamara, the Information Sharing Environment Program Manager, and Dr. Carter Morris, Director for Information Sharing and Knowledge Management, Intelligence and Analysis from the Department of Homeland Security. It has been my privilege over the past many months to work with these professionals and others as we seek to craft an outcome that matches both the letter and spirit of the task before us.

I join them today to discuss our collective efforts to develop a standardized framework for marking, safeguarding, and sharing "Controlled Unclassified Information" (CUI), or as it is more commonly known, "sensitive but unclassified" information.

On December 16, 2005, the President issued the "Guidelines for the Information Sharing Environment" as mandated by the Intelligence Reform and Terrorism Prevention Act of 2004. These Guidelines, among other things, set in motion a process for standardizing the handling of controlled unclassified information.

My nearly 24 years in the intelligence community have largely been served in an environment where I dealt almost exclusively with classified national security information. While those regimes could be complicated and required great discipline and attention to detail, by comparison they are far less challenging than my experience has been in working to organize a functional CUI framework. This is not because of a lack of commitment, focus and creativity in trying to address that framework, but because of the myriad of issues and interests that one encounters in the transitional world of information between what is controlled and what is not.

It is essential that we get it right, because it is information in this environment that can be of greatest utility when we need to share across a broad range of interests and constituencies. This framework provides a measure of protection for sensitive information to reassure those who might seek to hold such information in a classified or overly restrictive regime, which would deny others access and cause us to fail on our "duty to provide."

From an FBI perspective getting it right is essential. The Information Sharing Environment, which is the lifeblood of our mission, spans the range from classified national security information to fully open source. We must have the capacity to interpose information from all of these regimes and do so in a dynamic manner. We must have the ability to rapidly move information across security boundaries and into environments that make it more readily available and therefore of greater value to the broadest set of players. And across all of our partners, we must have a framework that allows for an immediate and common understanding of information's provenance and the implications that imparts. We must make the sharing of CUI a benefit, not a burden—especially on State, Local and Tribal police departments who would be disproportionately affected if asked to sustain a complex and expensive control framework. We must manage information in a way that sustains the confidence of people and organizations who share information that puts them at risk. Most important of all, we must respect the power of that information and the impact it holds for the rights and civil liberties of the American people who have entrusted us as its stewards. That also means that we must never use "control" as a way to deny the public access to information to which they are entitled.

For the FBI, achieving a streamlined CUI framework is much more than establishing a process, it's about shaping mindsets so we can fully shift from "need to know" to "duty to provide." This shift does not diminish our responsibility to properly protect the privacy rights and civil liberties of all Americans. It does not set up a framework that puts at greater risk our sources and methods and it does not compromise our capacity to conduct both an intelligence and law enforcement mission with full vigor and impact. Rather, this framework seeks to level the information sharing playing field through a common lexicon and a shared understanding of goals.

Unfortunately, the present set of policies and practices make it extremely difficult for well meaning individuals to act responsibly, appropriately and completely in this regime. There are well over 100 separate markings for CUI and there is no easy way for the recipient of information bearing an unfamiliar marking to find out what that marking means. Moreover, the same marking means different things in different parts of the Federal Government.

The FBI, working in close coordination with the Department of Justice, have jointly drawn upon the experience and the wisdom of state and local law enforcement personnel to help us understand better what kinds of CUI policies would be most helpful to them as we strive to share information without compromising either privacy or operational effectiveness. The Criminal Intelligence Coordinating Council (CICC) of the Global Justice Information Sharing Initiative has played an active role in advising us on this matter, including the convening on December 6, 2006 for an all day meeting to discuss the practicability at the state and local level of various proposed "safeguards" for CUI. I would like to acknowledge here the particularly constructive role played by the CICC Chair, Col. Bart Johnson of the New York State Police. Col Johnson is forthright in explaining what Federal policies would be most helpful in enabling state and local law enforcement to play their part in preventing terrorism, but he is also sophisticated in his understanding of the many other factors that must be taken into account.

In our view there are three aspects of the current draft framework that are particularly important:

1. Every marking that appears on any CUI document in the future must have a clear and unambiguous meaning. There should be a website—accessible over the Internet to everybody—on which the approved markings are defined, and no markings should ever be used that are not defined on this website. This will mean that recipients of shared information who want to do the right thing will easily be able to find out what protective measures are expected of them. I believe that this change will both increase sharing and decrease the risks of sharing.
2. All CUI information must be marked with a standardized level of safeguarding. For most CUI this safeguarding will be no more than ordinary prudence and common sense—don't discuss CUI when you can be overheard by people you don't intend to share it with, store it in an access controlled environment, as needed protect it with a password.
3. All CUI information must be marked with appropriate dissemination guidance so that recipients can easily understand what further dissemination is permitted.

All of us who have been part of this process wish we could have moved more quickly in reaching the point where we are today, but I believe the investment of time, the level of effort and the openness and commitment that has marked our dialog has done justice to the expectations of the American people.

Thank you for time, I look forward to answering your questions.

Ms. HARMAN. Thank you very much. We are impressed that there is a minute and a half left over. You win the prize, Mr. Murphy.

[Laughter.]

Well, I do apologize for rushing Ambassador McNamara. He has important things to tell us. But unless we adhere to this format, we don't give adequate time to ask questions and to respect the fact that we have a second panel of witnesses and also probably that we are going to have to recess for votes at some point during this hearing.

Well, I thank you all for your testimony.

And I will now recognize myself for 5 minutes of questions, and I will strictly adhere to the time.

Dr. Morris, I was sending DHS a message through you about frustration with the lack of progress on the ITACG and the inclusion of state, local and tribal representatives in the preparing of analytic products that is hopefully going to give those state, local and tribal authorities information they need in a timely way to know what to look for and what to do.

Every terror plot is not going to be hatched in Washington, D.C. where we might have adequate FBI and federal resources at the ready. I don't believe that for a minute, and I know no one on this panel does.

So I am sending this message that it is absolutely critical for DHS to spend more time supporting the inclusion of numerous state, local and tribal representatives in the ITACG and to stand up the ITACG promptly. We don't understand any reason for delay. I am speaking for myself. I have a feeling that the chairman is going to speak for himself shortly on this same issue.

And the way to do it right is the way Ambassador McNamara, working with you and state and local and tribal authorities, has come up with this proposal. So there is a positive example to learn from, and I hope that DHS, through you, is going to learn.

Are you going to learn?

Mr. MORRIS. I think that we are all committed to bringing state and locals into this activity. I can tell you personally it has always been my objective to do that. I have a meeting with my staff this afternoon on how we do this.

I think the challenge has been, the delay is that, in a sense, establishing the infrastructure for doing this kind of thing is more challenging than we would all like to have, but there is no lack of commitment, and we will move forward aggressively. And that is what we are doing.

Ms. HARMAN. Well, I hope that is true. Some of us thought that these folks could just be included in the NCTC itself, and then we were told we need a separate entity. Now you are saying setting up a separate entity has problems. I think the principle is the critical piece, and so let's not create problems with the second entity if it is a problem. Let's just move forward on the principle.

Mr. MORRIS. We agree. No, absolutely.

Ms. HARMAN. Sure. Okay.

Ambassador McNamara, I did rush you and you really didn't get a chance to lay out how this is going to happen. We all get it that the White House hasn't approved your proposal. We are hopeful that it will be approved. Surely, the other two witnesses were saying positive things about it, and we have been briefed, the members of this committee, by you on it, and we are positive.

Could you put on the record how this is going to happen, what the governance structure will look like, and could you address the issue of whether you need legislation to accomplish this?

Obviously, it makes no sense to have a brilliant proposal that no one follows, so I am sure you have already—I know you have already thought about this, and I don't think we have testimony yet on the record about how this will get adopted across the federal government.

Mr. McNAMARA. Yes, Madam Chairman. First of all, how: Right now the committee that I am chairing is putting in what I hope is final form a series of recommendations that will be a report to the president. He has asked for that report. It is known as guideline three, and we will be responding to that in, I expect, within a month or two, say, by the end of this quarter.

We will send forward for review by the interagency process—that means deputies, principals and then sent to the president—a series of recommendations. It is not a study, it is not an investigation. What it is, is a series of policy recommendations for changing the current system and instituting a new regime called, CUI, as I mentioned.

Second, you asked about the——

Ms. HARMAN. The need for legislation.

Mr. McNAMARA. For legislation.

Ms. HARMAN. To make certain there is compliance.

Mr. McNAMARA. Correct. There is in fact a group, a subgroup of this committee that has been looking at the legislative history of SBU and what might be necessary in the way of legislation for the implementation of a new regime.

It is headed by the Department of Justice, and we expect, once we have given them the final version of this, that they will come back to us with recommendations, and we will include those recommendations with the other recommendations. But those recommendations can't be made until they look at the product that we are telling them that we want implemented. And then they will give us their opinion as to whether or not legislation is needed.

On whether legislation is needed to get acceptance of this, the answer, I think, is, no. The president has asked for this, he wants it, and he will review it, I think, with dispatch.

Ms. HARMAN. I thank you for your answers. My time has expired.

I would just alert you and the public listening in that we are considering legislation here on the issue of over-classification, which Dr. Morris spoke to briefly, as well as this issue. We think it is absolutely critical that we have understandable and clear rules for what information is protected and what information is shared. Otherwise, we think, we are not going to be able to get where we need to get, which is to block Al Qaida plots coming our way in real-time.

I now recognize the ranking member of the subcommittee, the gentleman from Washington, for 5 minutes for questions.

Mr. REICHERT. Thank you, Madam Chair.

Just to follow up on the chairwoman's last question, governance and legislation, I was taking notes during your testimony and didn't find it in your written testimony, but you mentioned 280 pieces of legislation or ordinances and then another 150——

Mr. McNAMARA. Regulations.

Mr. REICHERT. —regulations.

Is the group in DOJ, are part of their tasks to take a look at those 280 and 150 to see——

Mr. McNAMARA. Yes, indeed. In fact, they were the ones who came up with those numbers.

Mr. REICHERT. Oh, okay.

Mr. McNAMARA. They did a research project to find out what legislation created the current SBU system and what regulations were adopted subsequently after the legislation was passed to implement the requirements of the legislation. That is where that comes from, from that group.

Mr. REICHERT. Because I can see that maybe some of what we could do, Madam Chair, is pass a law eliminating some of these rules and regulations that might be inhibiting you in accomplishing that task.

Mr. McNAMARA. Let me note that the vast majority, I believe, not having looked at all of them, but I have been told that the great majority of those simply require controls without going into detail as to what control mechanism should be put on specific kinds of information. The details of what controls were put on were determined by the regulations. And, therefore, it is the opinion of this group at this point that many of those legislative mandates require just a change of the implementing regulations rather than go back and change the legislation.

But the definitive answer will only come when we have a final set of recommendations that we can hand to the lawyers.

Mr. REICHERT. Great. Good. The subcommittee would be happy to be working with you on those changes.

I wanted to ask Dr. Morris, you mentioned as a part of the DHS mandate that you have, in that statement that you read, it talks about appropriate state and local personnel, which includes the private sector.

How do you define "appropriate"? Who does that include?

Mr. MORRIS. That is an interesting question. As part of my talks, I have talked about that word exactly, because it was written in there. I think that is something we have to work with the state and locals. The program that we currently have is certainly focusing on the fusion centers that operate at the state level and at the local ones that have that.

We believe that in the DHS program right now, that is where we are focusing our efforts and then working with the people in those fusion centers to understand where it needs to go beyond that.

One of the things that I have actually talked to some people who worked for me for awhile is, how do we define, in working with the fusion centers, what are the other distribution methods that need to be there? Who else has to get the information in order to act?

Mr. REICHERT. Yes.

Mr. MORRIS. I think that is the key thing. But right now our focus is through the fusion centers and working with the FBI and the activities that they do in the JTTF.

Mr. REICHERT. Good. Well, I think we all know from our experience that there are a lot of people who think they are appropriate, and that is the tough part is letting some people that they are not.

Also, we talked a few days ago, Ambassador, about cultural change as it relates to gaining trust and training, and it is also something that Mr. Murphy mentioned.

I kind of know where you are at on that, Ambassador, but I was hoping maybe Mr. Murphy might comment since you mentioned it in here, in your opening statement. The cultural change, in your opinion, is the need to know versus the need to share. So I think

you nailed it when you said that. How would you say we are going to reach that goal?

Mr. MURPHY. I wish I could take credit for that.

What really brought it home for me was when I was supporting a military operation as part of my responsibility at NSA, and afterwards we were doing a hot wash, and a Marine infantryman who was working as part of the front end operational activity told me, "What makes you think that you have my perspective? What makes you think you can make judgments about what I need to know and don't need to know? You need to understand my environment better and work within my environment."

That has resonated with me, particularly after 9/11, and the decisions I had made that made good sense at the time but, frankly, were parochial and limiting. I think this moves toward exposing our customers to the information that we have and letting them help us shape the message and shape the way it is delivered so the people that they represent is absolutely critical.

And so changing the mindset, at the end of the day, is more important than any process thing that we do, because if the mindsets change, the processes will really take care of themselves.

Mr. REICHERT. I appreciate that answer very much, and we are all three on the same page.

Ms. HARMAN. The gentleman's time has expired. I appreciate that answer very much too.

I now yield 5 minutes to the chairman of the full committee, Mr. Thompson of Mississippi.

Mr. THOMPSON. Thank you very much, Madam Chairman.

Good answer, Mr. Murphy.

Dr. Morris, if we implement CUI framework, do you think we can get DHS to come along?

Mr. MORRIS. Well, I don't think there is any problem with us coming along. I think that the only issue that I believe that we need to address in the end is going to be, how do we make sure with any new system we come up with that we build the trust in that system and the trust in the markings, the controls, the disseminations that are specified by that?

One of the big challenges for us in DHS has been working with the private sector, particularly, in the sharing of threat information on our critical infrastructure. And what we are dedicated to do under the new system is to make sure that whatever it says on the top of the piece of paper along an electronic message that people trust that system. And we think that is so critical in working with the private sector.

Mr. THOMPSON. And so do you think we can get our ICE, CBP, TSA to buy into it also?

Mr. MORRIS. I didn't say it was going to be easy. Yes, I do. Actually, I do. I think that we have socialized the proposal within the department. We haven't gotten back major pushbacks on it. I think people are still wondering how they are going to implement it, but in principle, yes, we have gotten acceptance.

Mr. THOMPSON. Ambassador, what participation have we gotten in the development of this new framework from the private sector? Did you have any discussions with any private sector stakeholders or anything?

Mr. McNAMARA. Yes, we have. We have been in consultation with them. There is a committee that the Department of Homeland Security has formed with private sector partners to examine many issues related to homeland security, not just this issue of the SBU and CUI. And we have gone over with them in some detail various aspects of this proposed and this recommendation for CUI that would affect the private sector in particular.

We have had telephone conferences, we have had meetings with them here in Washington. They are about, I think, within a few days or a week to send in some final comments on the CUI proposal as well as some other proposals that they have been looking at to, I think, the chair of that committee or that group, the assistant secretary for infrastructure protection at the Homeland Security Department, Bob Stephan.

And my understanding, from phone conversations, et cetera, is that they will be favorably disposed. They believe that their needs will be met by this new proposal for CUI.

Mr. THOMPSON. I yield back, Madam Chair.

Ms. HARMAN. Thank you, Mr. Chairman. We have been so efficient that I would ask Sheriff Reichert if he has an additional question, maybe one, and then we will move to our second panel.

Unless you do, Mr. Chairman.

Mr. THOMPSON. I have no further questions.

Mr. REICHERT. I would like to just give Dr. Morris a chance to address the cultural change. I noticed you had your hand up and you might have a comment there.

Thank you, Madam Chair.

Mr. MORRIS. I was just going to make a comment. I was on another panel recently and we were talking about information sharing, and there was a representative from private industry who came to the panel and basically said that approaching information sharing the way we are doing it now is going to fail, because it doesn't address the issue of discovery. And that gets back to the key point that you were making is that we have to put in place a system that promotes discovery of information, find the people out there who need it.

And then that is an area that we really need to start and continue. It struck a note with me, and I certainly agreed with what I heard.

Mr. REICHERT. Madam Chair, if I could just quickly follow up. The public disclosure issue, as you mentioned discovery, is also one that I think the FBI might have to handle and deal with, isn't that true, all three, nod your head?

Thank you.

Ms. HARMAN. Well, I thank the witnesses and do agree with the ranking member that building trust is the key to making all of this work. Without that, discovery won't happen, changing cultures won't happen and getting information, accurate and actionable information in real-time won't happen.

This is, as far as I am concerned, the critical mission for this subcommittee to drive home.

Ambassador McNamara, I hope when you leave this room you will call the White House and ask them what minute they are

going to approve your guidelines so we can get on with this. Right? Good. I know the phone number.

[Laughter.]

All right. This panel is excused. Thank you very much.

Thank you very much, all.

Are we now set up? Yes, we are. Counsel can take a seat next to me.

I welcome our second panel.

Our witness, Mark Zadra, serves as assistant commissioner, Florida Department of Law Enforcement, and is a 29-year veteran who has served in many leadership positions. Among them was overseeing the development and implementation of various intelligence and information technology systems.

He served as special agent supervisor of the Domestic Security Task Force prior to his appointment to chief of office of statewide intelligence in 2002 and subsequently to special agent in charge of domestic security and intelligence. And as we heard, he welcomed 600 people to Florida recently to have a conference on the critical subject of fusion centers.

Without objection, Mr. Zadra's full statement will be inserted in the record.

And I would now ask you to summarize in 5 minutes.

**STATEMENT OF MARK ZADRA, ASSISTANT COMMISSIONER,
FLORIDA DEPARTMENT OF LAW ENFORCEMENT**

Mr. ZADRA. Thank you, Madam Chair and distinguished members of the committee. I am pleased to speak to you today about the importance of common federal information sharing protocols and the impact that they have on the state, local and tribal governments.

Prior to 9/11, law enforcement agencies at all levels had little need to share sensitive information with non-law enforcement agencies. We had a generally accepted practice for sharing with one another, but because local and state law enforcement had minor involvement in the counterterrorism arena, we had limited experience with classified information. Little consideration was also given to sharing information outside of law enforcement, and particularly with respect to the private sector, it was generally not done.

The paradigm shifted after 9/11 when it became known that 14 or more of the hijackers had lived, had traveled and trained in the state of Florida while planning their atrocities. One month later, Florida experienced the first of several nationwide deaths from anthrax, which once again terrorized our nation.

In light of these grim realities, we recognized that local, state and tribal resources, together with a whole new set of non-law enforcement partners, including the private sector, represent the frontline of defense against terror and our best hope for prevention.

Over the years, since 9/11, collectively, we have made great strides in overcoming the cultural barriers to information sharing. Despite many successes and a new cultural that encourages information sharing, barriers that impede the establishment of the desired national information sharing environment remain.

Perhaps the single largest impediment is the lack of nationally accepted common definitions for document markings and standard

policy procedures for handling, storing and disseminating non-classified information.

Some states like Florida have open record laws, while other states impose very restrictive requirements and afford broad protections from release. Florida's reputation is that of an open record state, and it is widely known.

Exemptions provided by Florida's public record law are insufficient to protect against public disclosure of all types of sensitive information. The fear that sensitive information may not be protected under state law has a chilling effect on the free flow of information from out-of-state agencies and non-governmental to and from Florida.

We also believe that a lack of a standard definition results in federal agencies over-classifying information in an effort to protect it.

Developing and implementing a nationally accepted designation will provide Florida and other states with the justification that they need to encourage modification of state laws so that sensitive information can be protected.

Florida supports the implementation of the controls, unclassified information framework to replace the existing, sensitive but unclassified designation. Implementation of the new standard will involve varying degrees of physical and legislative impacts. However, it is my opinion that acceptance will be facilitated if the guidelines are straightforward and delivered in clear and concise language that there is a single, nationally accepted, encrypted communication standard and system, which can also be used by non-law enforcement homeland security partners and that that be designated.

The fiscal impacts are mitigated through the use of grants for the training and awareness programs and reprogramming of systems to allow this new framework.

And then implementation timelines need to consider the need to change policies and laws, purchase new equipment, do programmatic changes and to do the training that I referenced.

Federal agencies are now providing state and local agencies with significant amounts of threat information. Much of the information that is still needed, however, is classified at the national level in order to protect methods, means and collection and national security interests. Under most circumstances, however, we do not need to know the identity of the federal sources, nor the means, nor the methods of intelligence collection, only whether the information is deemed to be credible and specifically what actions that they want state, local and tribal authorities to take.

Florida believes the implementation of state regional fusion centers is the key to the establishment of the desired information sharing environment. These centers bring properly trained and equipped intelligence professionals with appropriate clearances to connect the puzzle pieces and disseminate actionable intelligence.

The problem remains that, unfortunately, most of the operational components at the state and local level that may benefit from the information and would otherwise be available to report on indicators and warnings we observed in the field will never have access to this information because of the classification.

Tear line reports forwarded to fusion centers can help address this particular concern. So state, local and tribal law enforcement,

in addition to other discipline partners and the private sector, can receive information that they can act upon.

Madam Chair and members of the subcommittee, thank you for the opportunity to appear and testify before you. I can assure you that the state of Florida is encouraged by your interest in facilitating an enhanced information sharing environment across the nation. It is my hope that the testimony and the understanding of Florida's desire to be a strong participant in the flow of critical, sensitive information and intelligence nationally will be help on your endeavor.

And, ma'am, if I may take 15 more seconds. I want to, from a state perspective and probably on behalf of Colonel Johnson, to thank you for the recognition and the gratefulness on behalf of the nation for the agency's loss of their trooper, the New York state trooper, the New York state police and lost his family and agency. And thank you for recognizing the sacrifice of the state and local and tribal multidisciplinary partners that are also part of this fight on terror.

Thank you.

[The statement of Mr. Zadra follows:]

PREPARED STATEMENT OF ASSISTANT COMMISSIONER MARK ZADRA

Good morning Madam Chair and distinguished members of the Subcommittee.

My name is Mark Zadra and I am a 29 year member of the Florida Department of Law Enforcement (FDLE). FDLE is a statewide law enforcement agency that offers a wide range of investigative, technical and informational services to criminal justice agencies through its seven Regional Operations Centers, fifteen Field Offices, and six full service Crime Laboratories. Our primary mission is to promote public safety and strengthen domestic security by providing services in partnership with local, state and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. FDLE utilizes an investigative strategy that comprises five primary focus areas including Violent Crime, Major Drugs, Economic Crimes, Public Integrity and Domestic Security.

I was recently appointed as FDLE's Assistant Commissioner of Public Safety Services however, prior to that appointment I served as the Special Agent in Charge of Domestic Security and Intelligence and the state's Homeland Security Advisor. In those roles I have overseen the development and implementation of various intelligence and information sharing programs and systems for FDLE and subsequently for the State of Florida. I have also overseen the development and implementation of the prevention component of Florida's Domestic Security Strategy and Florida's implementation of national information-sharing initiatives such as the Homeland Security Information Network (HSIN) and Florida's fusion center. I have further been an active participant on the Global Justice Information Sharing Initiative—Global Intelligence Working Group (GIWG). The goals of the GIWG include seamless sharing of intelligence information between systems, allowing for access to information throughout the law enforcement and public safety communities, creating an intelligence sharing plan, determining standards for intelligence sharing, developing model policies, determining training needs, and creating an outreach effort to inform law enforcement of the result of this effort. Over the last ten months I have been afforded an opportunity to provide input to the GIWG regarding the development of the recommended common protocols for sharing and protecting sensitive information and intelligence among multiple agencies with a role and responsibility in homeland security.

I am pleased to speak to the Committee today about the importance of common federal information sharing protocols and the impact they have on state, local and tribal governments.

Prior to 9/11, law enforcement agencies at all levels had little need to share sensitive information with non law enforcement agencies. We had generally accepted practices for sharing information with one another but, because local and state law enforcement had minor involvement in the counterterrorism arena, we had limited experience with federally classified information. Little consideration was given to

sharing sensitive information outside the law enforcement community, and sharing information with the private sector was generally not done.

The paradigm shifted after 9/11 when it became known that fourteen or more of the hijackers had lived, worked, traveled and trained across Florida while planning the atrocities they would ultimately commit. In their daily activities they left many clues that, if viewed together, may have predicted the plan and given authorities an opportunity to avert the catastrophic consequences. One month after the horror of 9/11, Florida experienced the first of several nationwide deaths from Anthrax which once again terrorized our nation. In light of these grim realities, we recognized that local, state and tribal resources together with a whole new set of non-law enforcement partners including the private sector represent the front line defense against terror and our best hope for terror prevention. Appropriately shared information is the key weapon in moving from the role of first responder to that of *first preventer*.

Sharing information with agencies such as health, fire, emergency managers, and even non governmental entities with a role in the fight against terror presented new challenges, not just the inherent cultural ones, but those relating to law, policy/procedure, technology and logistics. Over the years since 9/11, collectively, we have made great strides in overcoming the cultural barriers to sharing information. In Florida, through our Domestic Security Strategy and governance structure, we routinely work with and share information across all entities that have a role in protecting the safety and security of our citizens.

Despite these successes and a new culture that encourages information sharing, barriers that impede the establishment of the desired national Information Sharing Environment (ISE) remain.

Common Document Markings and Dissemination Protocols

Perhaps the single largest impediment to an effective national ISE is the lack of nationally accepted common definitions for document markings and standard policy/procedure for handling, storing, and disseminating non classified information. Sensitive but unclassified information, which is routinely received from federal and other state agencies, is needed by state, local, tribal and private sector partners that have a duty and responsibility to utilize it to provide for our safety and security. Consistency in definition and protocol is paramount to both fully sharing useful and actionable information, and protecting information that should not be shared.

Some states, like Florida have open record laws that mandate revealing information compiled by governmental agencies unless a specific "chapter and verse" exemption or confidentiality provision applies. Other states impose very restrictive dissemination requirements and afford broad protections from release to those without a need to know. Florida's reputation as an open records state is widely known. While Florida law exempts certain information from public disclosure, the most likely exemptions applicable to the type of information that I am discussing are limited to criminal intelligence/investigative information and information that pertains to a facility's physical security system plan or threat assessment. Exemptions provided by Florida's Public Records Law are insufficient to protect against public disclosure of all types of sensitive information needed by Florida's domestic security partners. For example, there is no specific exemption in Florida's public records law for information provided to Florida by a non Florida agency unless it is intelligence or investigative information both of which have fairly narrow definitions under Florida law. The fear that sensitive information may not be protected under state law has a "chilling effect" on the free flow of important information from out of state agencies and non governmental entities to and from Florida. We also believe that the lack of a standard designation results in federal agencies over classifying their information in an effort to protect it. Information and intelligence sharing partners need to know, with certainty, that the information they share will be appropriately protected. At the same time, we understand there must be appropriate limits on what is removed from public scrutiny and review, and a balance achieved between properly informing the public and ensuring the safety and security of our state and nation.

Developing and implementing a nationally accepted designation, with clear and appropriate handling and dissemination standards for sensitive information, will provide Florida and other states with the justification they need to encourage modification of state laws so that sensitive information can be protected in compliance with an accepted national standard.

Fortunately, there appears to be a workable solution to the concerns I have identified. Florida supports the implementation of the Controlled Unclassified Information (CUI) framework to replace the existing Sensitive But Unclassified (SBU) designation. The SBU designation contains numerous confusing designations used to mark

unclassified information. The recommended CUI framework streamlines existing designations and provides handling requirements that facilitate wide distribution among law enforcement, homeland security, other government sectors and the private sector. We strongly believe that the information sharing environment mandated by Presidential Guideline 3 cannot be fully achieved without the implementation of a model such as the CUI framework. In the absence of common protocols, existing classification schemes will continue to be over utilized and/or improperly utilized, resulting in the inability of persons who receive information to adequately distribute it to those with a duty and responsibility to take action to protect our citizens.

We believe that the recommendations made by the Sensitive But Unclassified Working Group reflect workable solutions that could be accepted and replicated by most states. As a state representative I have been afforded an opportunity to review and comment on these recommendations during their formulation. I have also had the pleasure of personally meeting with Ambassador Thomas E. McNamara, Office of the Program Manager for the Information Sharing Environment and espousing Florida's views with respect to this and other information sharing topics.

Implementing CUI

In the absence of federal guidance and standards, many states, including Florida, have already expended resources in building systems and programs to fill the information needs of their consumers. Implementation of the new standard will involve varying degrees of fiscal and legislative impacts, however it is my opinion that acceptance will be facilitated if:

1. Guidelines are straight forward and delivered in a clear, concise language;
2. A single, nationally accepted, encrypted communications system and federal information sharing encryption standard that can be used by non law enforcement homeland security partners is designated;
3. Fiscal impacts are mitigated through grants for training and awareness programs, as well as for new equipment and system re programming; and
4. Implementation timeline considers the potential need for state, local, and tribal governments to:
 - a. Change policy and/or rules to comply with new information dissemination requirements;
 - b. Purchase new equipment and/or system programming changes; and
 - c. Train appropriate personnel in markings, handling, storage and dissemination requirements.

For Official Use Only Tear Line Reporting

In response to post 9/11 criticism regarding failure to share information vertically and horizontally across the spectrum of homeland security partners, federal agencies are now providing state and local agencies with significant amounts of threat information. Much of the information that is still needed, however, is classified at the national level in order to protect sources, methods and means of collection and national security interests. State and local law enforcement fully understand and appreciate the need to protect certain information and restrict dissemination to only those with a need or right to know. Under most circumstances, however, we do not need to know the identity of federal sources or means and methods of intelligence collection—only whether or not the information has been deemed credible and specifically what actions that the state, local and tribal entities should take.

Florida believes the implementation of state and regional fusion centers is key to the establishment of the desired Information Sharing Environment. These centers bring properly trained and equipped intelligence professionals with appropriate clearances to connect the pieces of the puzzle and disseminate actionable intelligence. The problem remains that once the classified material is fused with the non classified information from which analysis is performed, the information takes on the restrictions with the classified information which significantly narrows to whom and how it can be shared. Unfortunately, most of the operational components at the state and local level that may be benefit from the information, and would be otherwise available to report on the indicators and warnings being observed within the field, will not ever have access to this information. Tear line reports forwarded to fusion centers can help address this particular concern so that state, local and tribal law enforcement in addition to other discipline partners and the private sector receive information that they can act upon.

In conclusion, I would like to compliment our federal partners for recognizing the value of state, local and tribal representative's expertise and allowing input on such a critical initiative prior to its implementation. This has not always been the case, but is a testament to the positive change in the information sharing culture and established and improved partnerships. I have been honored to be a member of the

Global Intelligence Working Group and would like to acknowledge the work done by those professionals under the guidance of their Chairman, New York State Police Deputy Superintendent, Bart Johnson.

Lastly, Madam Chair and Members of the Sub Committee, thank you for the opportunity to have appeared and testified before you today. I can assure you the State of Florida is encouraged by your interest in facilitating an enhanced information sharing environment across the nation. It is my hope that this testimony and the understanding of Florida's desire to be a strong participant in the flow of critical sensitive information and intelligence nationally will be helpful in your endeavor.

Ms. HARMAN. I thank the witness for your testimony and now yield myself 5 minutes for questions.

Let me say, first, Mr. Zadra, that I think we need to bottle you. I am not sure what that process could involve, but I would like to a bottle of you to sit on Charlie Allen's desk and I would like a bottle of you to sit on the desk of the appropriate people at the CIA who have a great role to play in our present classification system.

And I definitely want a big bottle of you to be sitting on Fran Townsend's desk in the White House, as we move forward. Because it is absolutely critical, as you said, that you have timely information. And we have both classification and pseudo-classification systems that are making that more difficult than it should be.

No one is arguing about the need to protect sensitive sources and methods. I served for 8 years in the House Intelligence Committee, and I think I get it, but I haven't found a defender, and I would disagree with such a person if I found one, who says that our present system works well. It doesn't, it is broken, and this is hearing is about how to fix at least a portion of it, and this subcommittee will focus on trying to fix as much of it as we can get our arms around.

I want to ask you about a specific situation. I don't think anyone in the country and most people around the world missed the tragic events at Virginia Tech last week where 32 students and faculty lost their lives. Initially, it was not known who the shooter was. It turned out to be, we think, a mentally ill student acting alone.

But I want to ask you, from your perspective, what were you thinking about when that information came over the wire? For example, were you thinking, is this a terrorist plot, is this the first phase, is this going to roll out in some of my universities in Florida?

And what information were you able to get in real-time as you had those thoughts, and from whom?

Mr. ZADRA. Madam Chair, I can assure you that the state of Florida, there is not an incident that happens within our state, whether it is an accident of hazardous materials on a roadway or anything across the country, our mindset initially is first to determine whether or not it has a potential nexus to terrorism. I think we all learned a lesson after 9/11.

Certainly, when this happened our immediate thought, the Florida Department of Law Enforcement has protective operations detail for our governor and also for our legislature and cabinet. And we, of course, when we first heard the news, were concerned, did we have a nexus to anything within our state and our particular universities and colleges that we needed to also be concerned with.

Fortunately, because of the fusion center concept now, we have an embedded Department of Homeland Security analyst within our

state fusion center. Very immediately two things happened. We reached out immediately, through our DH analyst, to the national operations center, and we were advised very quickly that there was no known nexus to terrorism. Of course, it was still unfolding at that time, but there were no initial indicators.

The second thing that happened, which I think is proof positive about the fusion center concept is that the Virginia fusion center began putting out information that was made available to the other state fusion centers. And that was extremely critical and beneficial to us.

I know the last thing that we would want to do as a state is to call and begin impacting the local law enforcement agencies that were responding to that tragic incident. They had their hands full. To have a state, a thousand or more miles away, calling and wanting to check to know the status of everything, it would be understandable that that could be an impediment to them.

But because of the fusion center there and to be able to reach out to them directly and with them providing updates to us, and I know the last I saw was update number six, I know at least six updates were provided from that fusion center to all fusion centers across the nation.

Ms. HARMAN. Well, that is a good news report. That is not a report you could have given a year or two ago, am I right?

Mr. ZADRA. Yes, ma'am, that is correct.

Ms. HARMAN. Fusion centers, which have been the subject of other hearings, are beginning to work. DHS does have personnel embedded in 12 of them. You are obviously one of 12. We are trying to help move more DHS people there, and I am just assuming that the products you saw also reflected, for example, FBI input, since they are typically a part of the fusion center. Is that correct?

Mr. ZADRA. Yes, ma'am, that was my understanding, that there was a cooperative effort. And let me add, too, that we are awaiting our FBI analyst. We will have an FBI analyst also embedded in our state fusion center. The member has just not arrived yet, but we are expecting that soon.

Ms. HARMAN. Well, I hope that does happen. I mean, the goal, again, is to get the right people and right information to the right places in real-time. Do you agree?

Mr. ZADRA. Absolutely.

Ms. HARMAN. I thank you very much, Mr. Zadra, and now yield 5 minutes to the ranking member for questions.

Mr. REICHERT. Good morning.

Thank you, Madam Chair.

First of all, you mentioned open record laws. I am from Washington state, was the sheriff there for a while. In 33 years of law enforcement, one of the frustrating things in working with the federal government, and you touched on, was sharing that information and as they shared it with the local sheriff's office in Seattle, it became subject to the public disclosure laws of the state of Washington.

Can you talk a little bit about that, how that discussion occurred within the framework of your involvement in discussing where one had the future of sharing information?

Mr. ZADRA. Yes, sir. In the state of Florida, we have some exemptions from public disclosure, and from our perspective there are usually three that we point to. One is active criminal investigation, the other is active criminal intelligence, and then the other deals with security plans, which include photographs, floor plans and things like that, of critical infrastructure.

While those are good, there is a hole, so to speak, with sensitive information, because now, after 9/11, we have a lot of different partners that we need to share with—health, fire, emergency managers. So a lot of the information that we get is not active criminal investigation, it is not active criminal intelligence, and it is not a floor plan, it is not a photograph.

For example, if we have mass prophylaxis from dealing with health issues and where that is stored and how it is transported, as we have hazardous materials come through our state, we want to alert our Florida highway patrol, we want to alert our motor carrier compliance, our Department of Agriculture, their weigh and inspection stations, of the flow of this.

Under our current public records exemptions, that information is not criminal investigative, it is not criminal intelligence, and it is not a security plan. We attempt to protect it under those type things, and we have been pretty much successful.

But to have a national framework that we—and I have talked to both our house and our senate in our state, and if we had a national framework that we could point to, to say, this is a nationally accepted, controlled, unclassified information that we could amend our state laws to provide those protections so that when we need to share with other states, they have confidence that the state of Florida, despite being an open records law state, that we can protect the information they share with us.

Mr. REICHERT. Very good. The last part of my question was going to address the last part of your answer.

I was also wondering what your opinion might be in this whole area of governance, because local law enforcement has difficulty at the state level, the sheriff's level and the police chief. Who is going to be in control of the information? The governance issue is a big one, as you know. It is always a huge issue.

How did that discussion play out in your discussion of SBU and all the players around the table? That governance issue is always touchy.

Mr. ZADRA. The state of Florida is a participant in the Global Intelligence Working Group under the global justice initiative, and so the state of Florida has been able to provide input. I personally have been able to review the recommendations and provide input to those.

I also served as homeland security advisor until most recently, and we have seven regional domestic security task forces that all have intelligence operations and components. So we have had discussions with those, and everyone agrees that this is a difficult, and we need a national standard.

We have awaited, of course, understanding the formal adoption of these before we have done a lot of pushing out to our state, because one thing that happens, while you want to have the input from your local state, one thing that has happened to us that en-

couraged our federal partners, it really needs to be done and it needs to be done right, so when we take it and share it, we can share it once, and it doesn't move, and it doesn't change.

One of the most detrimental things that has happened to us in the past is the rollout of new programs, and I have heard them described as, well, we were building this airplane on the fly.

To be honest with you, sir, I don't want to fly on an airplane that is being built while I am on it, as we are flying.

And so what happens is you push these things out to the states, the locals. The federal government begins to lose credibility because it continues to change and morph.

So, truthfully, from the state's perspective, what we have done is we would like to know that there are recommendations, we have provided input, and once we believe that they are close to being finalized, to be able then to really push that through our state framework.

Mr. REICHERT. Great. Thank you so much.

I yield. Thank you, Madam Chair.

Ms. HARMAN. Thank you, Mr. Reichert.

We have votes coming up shortly, but I do have another question or two, and so I hope you will join me in a second round of questions until we can adjourn the hearing for voting.

First of all, it is Mr. "Zadra"? Is that correct?

Mr. ZADRA. Yes, ma'am, but anything is fine.

[Laughter.]

Ms. HARMAN. Well, you are very flexible, but this is my second goof of the morning here, besides recognizing another witness out of order. I apologize to you, and we will now produce Zadra pills, which we are going to put in every federal office.

I surely agree with you, in answer to your last question, that it needs to be done right. But it also needs to be done now. Do you agree with that?

Mr. ZADRA. Yes, ma'am.

Ms. HARMAN. Okay.

Mr. ZADRA. If not, the state and locals, like we have done on many things in the past, we have implemented our own methodologies and that continues to lead to the confusion and interoperability between states. So you are correct. It needs to be right, and it needs to be done as soon as possible.

Ms. HARMAN. So we have the ambassador calling the White House today, and we will have approval later today. That would be nice, obviously. Then we need a forcing mechanism across the federal government.

My question to you is, would some funds for training help push this concept into the states? I know there are some other issues that you were just discussing with Mr. Reichert, but would training money be of use to you?

Mr. ZADRA. Madam Chair, absolutely, and the recommendation for Florida that we have made, particularly through the Department of Homeland Security, deals with the federal grant funding programs, and I know that you are highly aware of those different ones.

We would ask, because currently we fund our fusion center efforts through the Law Enforcement Terrorism Prevention Program,

we would ask, because the fusion centers are so critical to this entire effort, that there be thoughts, just as there are designated port grants or transit grants, that we designate fusion center grants. And I believe that the money in a fusion center grant is so tied to what we are talking about that we would use those funds in conjunction with the fusion centers to deal with how we would train how to use CUI.

Ms. HARMAN. Well, we are working right now on several proposals to push more money into fusion centers to help with local training, local involvement, also to get DHS people in every fusion center. I was confused about your answer before, probably my fault, about the Virginia Tech information. Your fusion center does or does not presently have a DHS person in it?

Mr. ZADRA. It does.

Ms. HARMAN. It does.

Mr. ZADRA. It has since January.

Ms. HARMAN. And that fusion center was what you contacted, and it got in touch with the Virginia fusion center; is that what happened?

Mr. ZADRA. Our state Florida fusion center made contact with the Virginia fusion center. Our Department of Homeland Security analyst made direct contact to the national operations center, which is the Department of Homeland Security. We went both ways.

Ms. HARMAN. So we had a real live example of information sharing, horizontally at the local level and vertically with the federal intelligence community; is that correct?

Mr. ZADRA. Yes, ma'am. That is not the first time. I think we continually see progress and movement. And, again, the creation of state and the regional fusion centers and then having our federal components embedded in those, I think, are the best things that we could be doing.

Ms. HARMAN. Well, we totally agree. We think that is one of the best things. We think another of the best things is to change the way we protect information so that we only protect what we need to protect and we share the rest of it, both on the classified side and the pseudo-classified or non-classified side. And that is why we are having this hearing. And I think you are on the same page; am I right?

Mr. ZADRA. Absolutely. I couldn't agree more.

Ms. HARMAN. I thank you again for your very valuable testimony, Mr. Zadra, and now yield for additional questions to the ranking member.

Mr. REICHERT. I just have two or three follow-ups. Thank you, Madam Chair.

How much of your budget is dedicated to homeland security efforts? Would you know the answer to that?

Mr. ZADRA. How much of our state budget or federal grant?

Mr. REICHERT. Your agency's budget.

Mr. ZADRA. Our agency budget? Not a tremendous amount, and the reason why is because our state legislature, and I can forward it to you later, if you would like, sir, our state statute that designates our domestic security efforts in Florida indicate that we are to maximize federal funding.

I believe that Florida has placed approximately \$25 million of state revenue into this. Florida, fortunately, because of the critical infrastructure landscape that we have, we have been treated very well from the national level. I mean, we would always want more, but Florida has been a recipient and last year was the third largest amount of federal funding from the Department of Homeland Security.

Mr. REICHERT. What is your agency's training budget? What percentage of your budget goes to training?

Mr. ZADRA. Sir, I don't know the answer to that. I don't have that with me today. I can certainly provide that as a follow-up to you. I do note that we also maximize our federal homeland security funds to deal with our training.

Mr. REICHERT. And to further follow up on the chair's question regarding funding, would it be helpful to you to have additional funds that would pay for backfill as you send people to training?

Mr. ZADRA. Yes, sir. To be honest with you, I am sure it would be greatly appreciated. I think I can say on behalf of the state of Florida, particularly from the law enforcement component, is that this is our mission. It is clear to us. This is just as important as responding to any burglary, rape, robbery, and we would do it if you didn't give us backfill.

I will say this from the fire side: The fire, we do provide backfill and overtime for them. Because when you take a hazardous material truck and you send them all to training, that is loss. So if you take one member and they don't have enough to have that team, so they have to backfill that. Law enforcement, we are a little bit different.

So I guess the best way to answer that, we would be happy to receive it and it would be a benefit, but I will assure you the state of Florida is going to do what is necessary, even if we did not have it.

Mr. REICHERT. Well, one of the things we talked about—this is the last question I have—is creating an environment of trust. And I just have to smile, still being probably new here in my second term, beginning my third year at the federal acronyms, so just today SBU, CUI, ISE, PCI, ICC. So when you talk about building trust and user friendly, the local cops really would like language they can understand, don't you agree?

Mr. ZADRA. Sir, interesting that you bring that up, as Governor Crist, our newly elected governor, his very first executive order was a plain language initiative in the state of Florida.

Mr. REICHERT. Yes. I think it is a great idea.

Mr. ZADRA. We concur wholeheartedly. It needs to be very plain, it needs to be simple. And no disrespect to our law enforcement officers who are obviously very confident, but it makes sense that whatever we do has to be simple so that we can assure it is done properly and that it will be utilized. If it is too complicated, it is not going to be utilized and we won't effect what we are after.

Mr. REICHERT. Well, certainly appreciate your time, and thank you for your service to your community.

And I yield back.

Ms. HARMAN. I thank the gentleman for yielding back.

The time for questions has expired.

I would just note to Mr. Zadra that I often say the dirtiest four-letter word in government is not an acronym; it is spelled T-U-R-F, and it has a lot to do with the subject we are discussing today. The hearing is adjourned.
[Whereupon, at 11:22 a.m., the subcommittee was adjourned.]

**MAKING DHS THE GOLD STANDARD FOR
DESIGNATING CLASSIFIED AND SENSITIVE
HOMELAND SECURITY INFORMATION
PART III**

Thursday, June 28, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 10:08 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chairwoman of the subcommittee] presiding.

Present: Representatives Harman, Langevin, Carney, Reichert and Dent.

Ms. HARMAN. The hearing will come to order.

I apologize to my colleagues and our witnesses for needing to be in two places at the same time, but the Energy and Commerce Committee is marking up the energy bill, and that includes things like plug-in hybrids, which are a huge issue for California. So I will, as soon as my BlackBerry goes off, have to go out; and Mr. Langevin will chair the hearing for a period.

But I would like to welcome our witnesses and welcome our panel and take a deep breath and launch. Good morning.

According to last Sunday's Washington Post, the Vice President is inventing his own classified and unclassified designations to keep his work products secret. My personal favorite—and I have never heard of this designation in my 8 years on the House Intelligence Committee—is, quote, treated as Top Secret SCI, unquote.

According to the Post, experts in and out of Government said Cheney's office appears to have invented that designation, which alludes to Sensitive Compartmented Information, the most closely guarded category of Government secrets. By adding the words "treated as", the Post noted, the Vice President seems to be seeking to protect his unclassified work as though its disclosure would cause exceptionally grave damage to national security.

The problem is that the Vice President and some other law enforcement and security agencies believe that they should decide which information they can keep secret, regardless of the law, rules or what the needs are of our local law enforcement community.

In my view, this is bad policy. But, not only that, it poses huge obstacles to our need to connect the dots in time to protect, to prevent or to disrupt the next terrorist attack against us.

I ask the question, what hope is there for the controlled unclassified information regime being developed by the program manager of the Information Sharing Environment at the DNI's office if we have agencies and parts of our White House that are going to continue to make their own decisions on what information they keep secret?

One of our witnesses today is a player, a participant, in the controversy involving the Vice President's office. Bill Leonard of the Information Security Oversight Office testified before this subcommittee this past March, and we welcome him back. At the prior hearing, he and other witnesses helped paint a picture of the consequences of abusing the classification regime and its outrageous costs to both taxpayers and our information-sharing efforts.

I am aware, Mr. Leonard, that the Justice Department is currently trying to resolve the issue between your office and the Vice President, and I anticipate that you may not be able to comment on the issue, but surely I personally admire your courage, and I think you are on the right side.

Mr. Leonard appears today to testify about what he believes the Department of Homeland Security should do to reduce the problems from overclassification and pseudo-classification.

And our other witnesses, each of our other witnesses, brings enormous expertise to this. Several of you have been witnesses before us before. All of you are people whom I talk to on a regular basis about what this committee should be doing to get the problem right.

Let me just state a few other tentative conclusions that we have reached after exploring this issue for some time.

Number one, the only way to insure that relevant homeland security information is shared between the Federal Government and its State, local, tribal and private sector partners is to create a classification and pseudo-classification system that is enforceable, understandable and applicable to everyone.

Number two, almost 6 years after 9/11, we should be treating far less information as classified.

Number three, fixing this should be a top priority.

Number four, classified markings are not—repeat not—to be used to protect political turf or hide embarrassing facts from public view. They should only be used to properly hide—if that is a good word—or protect sources and methods from public view because if those sources and methods are disclosed, people die and information dries up.

Indeed, a recurrent theme throughout the 9/11 Commission's report was the need to address the problems of over—and pseudo—classification to clear up a major stumbling block to dealing with terrorist threats.

While I hope that Congress will fashion a Government-wide solution, this committee, the Homeland Security Department and this subcommittee is a good place to start. We can try to figure out what Homeland Security should be doing, and we can hope that what we propose for the Homeland Security Department can become the best practices Government-wide.

As I mentioned, we have phenomenally good witnesses before us today; and I look forward to working with them, continuing to work

with them, and to working on a bipartisan basis with Sheriff Reichert getting this right.

I would like to extend a warm welcome to everyone and would now yield to the ranking member for his opening comments.

Mr. REICHERT. Thank you, Madam Chair; and welcome to all of you.

I have a couple of pages of prepared comments, but I am just going to read one paragraph, and then I am going to comment from more of a local perspective.

This subcommittee is to focus on the Department of Homeland Security and actions that they can do better in terms of overclassification, pseudo-classification. However, in crafting legislation, we must not lose sight of the fact that overclassification is a Government-wide problem, and that requires Government-wide solutions. I think really that kind of boils the whole thing down.

I just want to again comment from a local perspective. It has only been a little over 2 years since I came from the Sheriff's Office in Seattle. I had 33 years experience there, some working with the Federal officials, the FBI, Secret Service and DEA and ATF and you name it, from a detective's perspective in sharing information and working as partners in investigating crimes.

One of those crimes, as I mentioned in earlier hearings, is a well-known case called the Green River Murder Investigations, where we had nearly 50 to 60 Federal agents assigned to the task force. I operated there as the lead investigator from the middle 1980s into the early 1990s. We had difficulty obtaining information from the Federal agencies and agents that worked there with us, right alongside, side by side.

My partner, FBI agent Special Agent Bob Agnew, shared information with me because we built a relationship. We had a friendship where we trusted each other. But the agency itself classified the documents that were associated with our case at a level where I had no access to the documents in our own case. So this is back in the 1980s.

So when we finally come to make an arrest years later, 19 years later, while I then served as the first elected sheriff in 30 years in Seattle, I had the opportunity once again to oversee for 2 years the investigation of this serial murder case that solved 50 murders. Part of that investigation then required that we go back to the Federal agency, the FBI, and acquire the documents that they had produced during that investigation for discovery so that we could pursue charges against the suspect. They refused to give them to us. That is ridiculous, and it touches on the level that the Chair mentioned at a local level.

Really, it boils down to, look, cops on the street, the local cops, the local sheriff's deputies, the State Patrol, you know, the State agencies, and all the other Federal agencies, the guys and gals on the street do not care one iota about the Vice President and the politics of this stuff. What they want is a system in place where we can share information, where we can build that trust, that sort of friendship that Bob Agnew and Dave Reichert had back in the mid-1980s, where we could share the information vital to investigating a local crime.

Now, in today's world, after September 11th, vital to the security of this Nation, because, as we have all said over and over again in this subcommittee and in our full committee, the involvement of local law enforcement is critical in the protection of our country. And if we don't share information with our local agencies and we can't trust each other and build trust between local agencies and Federal agencies, this country's safety is at great risk.

So I know all of you are working hard to overcome this problem, but I wanted to share with you just one of my experiences in my 33-year career working with one Federal agency. I have other stories I could share with you that would illustrate this point, but I won't take the time this morning.

So I appreciate you being here this morning and look forward to your testimony.

Madam Chair, I yield.

Ms. HARMAN. I thank the gentleman for his comments and would note that other members of the subcommittee are reminded that, under committee rules, opening statements may be submitted for the record.

Ms. HARMAN. As mentioned, I welcome our four witnesses.

Our first witness, Mr. William Leonard, is the Director of the Information Security Oversight Office. The ISOO reports to the President and is responsible for policy and oversight of the Federal Government-wide security classification system and the National Industrial Security Program.

Mr. Leonard has testified several times before Congress about the need to break down the classification impediments to information sharing. Some of them were just graphically mentioned by Mr. Reichert.

Our second witness, and a very long-standing friend of mine, is Scott Armstrong, who is the Executive Director of the Information Trust, a nonprofit group that works toward opening access to Government information. He has been inducted into the Freedom of Information Act, FOIA, Hall of Fame—that is impressive; I hope you are wearing the medal—and was awarded the James Madison Award by the American Library Association.

Mr. Armstrong has been a Washington Post reporter, a member of the board of several nonprofits, is the founder of the National Security Archive of the George Washington University and co-author of a major book on the Supreme Court.

Our third witness, Suzanne Spaulding, is an authority on national security issues, including terrorism, homeland security, critical infrastructure protection, cybersecurity, intelligence, law enforcement, crisis management and issues relating to the threats of chemical, biological, nuclear and radiological weapons. She just knows everything.

She started working on national security issues on Capitol Hill over 20 years ago. More recently, she was the Executive Director of two congressionally mandated commissions, the National Commission on Terrorism, on which I was a member and where I met her, and the Commission to Assess the Organization of the Federal Government to Combat Proliferation of Weapons of Mass Destruction, which was chaired by former CIA Director John Deutch; and

she also was the chief of staff to the then minority on the House Intelligence Committee when I was the ranking member.

Welcome back, Suzanne.

Ms. SPAULDING. Thank you.

Ms. HARMAN. Our fourth witness, Mark Agrast, is a Senior Fellow at the Center for American Progress, where he focuses on the Constitution, separation of powers, terrorism, civil liberties, and the rule of law.

Prior to joining the Center for American Progress, Mr. Agrast was counsel and legislative director to Congressman Delahunt of Massachusetts. He serves on the 37-member Board of Governors at the American Bar Association, past Chair of ABA's section on Individual Rights and Responsibilities, and a former colleague of mine in law practice. Very, very knowledgeable about this subject.

Without objection, all the witnesses' full statements will be inserted in the record; and I would now urge you each to summarize, in 5 minutes or less, your principal points.

We do have a timer. You will see it. It will start blinking at you. But it will be much more productive if we can have a conversation here, not just having you read from a prepared text. And all of us are very eager to learn from you today.

**STATEMENT OF J. WILLIAM LEONARD, DIRECTOR,
INFORMATION SECURITY OVERSIGHT OFFICE, NATIONAL
ARCHIVES AND RECORD ADMINISTRATION**

Ms. HARMAN. Please start, Mr. Leonard.

Mr. LEONARD. Thank you, Madam Chair, Mr. Reichert, members of the subcommittee. I want to thank you for holding this hearing today and giving me the opportunity to appear.

Obviously, the ability and the authority to classify national security information is a critical tool at the disposal of the Government and its leaders to protect our Nation and its citizens.

As with any tool, the classification system is subject to misuse and misapplication. When information is improperly declassified or not classified in the first place, although clearly warranted, our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations can be subject to potential harm.

Conversely, too much classification, the failure to declassify information as long as it no longer satisfies the standards for continued classification, or inappropriate reclassification unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of Government.

In this time of constant and unique challenges to our national security, it is the duty of all of us engaged in public service to do everything possible to enhance the effectiveness of this tool. To be effective, the classification tool is a process that must be wielded with precision.

Last year, I wrote to all agency heads and made a number of recommendations for their consideration. Collectively, these recommendations help preserve the integrity of the classification system, while at the same time reduce inefficiencies and cost. They included things such as emphasizing to all authorized holders of classified information the affirmative responsibility they have under

the order to challenge the classification status of information they believe is improperly classified.

I also suggested requiring the review of agency procedures to ensure that they facilitate classification challenges. In this regard, agencies were encouraged to consider the appointment of impartial officials ombudsmen, if you will, whose sole purpose is to seek out inappropriate instances of classification and to encourage others to adhere to their individual responsibility to challenge classification as appropriate.

Also, I suggested ensuring that quality classification guides of adequate specificity and clarity are absolutely necessary in order to insure accurate and consistent derivative classification decisions.

In this letter, I also suggested ensuring the routine sampling of recently classified products to determine the propriety of classification and the application of proper and full markings. Agency inspector generals, for example, could be involved in this process.

Consideration should also be given to reporting the results of these reviews to agency personnel as well as to officials designated who would be responsible to track trends and assess the overall effectiveness of the agencies' efforts and make adjustments as appropriate.

Finally, I suggested that agencies need to ensure that information is declassified as soon as it no longer meets the standards for continued classification.

Again, thank you for inviting me here today, Madam Chair; and I would be happy to answer any questions you or the subcommittee may have.

Ms. HARMAN. Thank you, Mr. Leonard.

[The statement of Mr. Leonard follows:]

Ms. HARMAN. I just want to announce to all that I have to leave to return to this markup. I will try to get back. Mr. Carney will assume the Chair, because Mr. Langevin has to depart shortly. But we will hear testimony from all four of you, and then we will ask questions of all four of you.

Again, I would like to thank you all, but I would like to say to you particularly, Mr. Leonard, that you are in a tough fight, and your courage and integrity are very impressive. Thank you very much.

Mr. LEONARD. Thank you.

Ms. HARMAN. Without objection, I will now turn the Chair over to Mr. Carney.

Mr. CARNEY. [Presiding.] Thank you, Mr. Leonard, for your testimony.

Mr. ARMSTRONG. Thank you.

Mr. ARMSTRONG. I was intending to wish our chairwoman, Mrs. Harman, a happy birthday, as today is her birthday, but we can sing to her when she returns.

Mr. CARNEY. Not me. I want to get re-elected.

STATEMENT OF SCOTT ARMSTRONG, FOUNDER, INFORMATION TRUST

Mr. ARMSTRONG. I appreciate the opportunity to address these issues of classification and pseudo-classification at the Department of Homeland Security.

My views are my own, but I should note I have been working closely within the Aspen Institute to sustain a 6-year dialogue between senior journalists, editors and publishers and high-level Government officials from various national security agencies, including senior members of Congress and their staffs. We met from time to time with the Director of Central Intelligence and the Attorney General and ranking members of the various intelligence bureaucracies. The product of those meetings I think is an agreement that the goal is to have a well-informed citizenry that is assured of its safety, without sacrificing its liberty.

The lessons of 9/11 were focused on sharing more information within Government agencies, laterally across Government agency barriers, and among Federal, State, and local governments and with critical private industries, community first responders and the public at large.

The challenge for the Department of Homeland Security is not so much how to withhold information or secrets from the public but how to share information so as to promote our security. For once, the Government's first mission is not to silence leaks but to effectively share official information outside of its usual constraints.

The discipline of controlling information needs to give way to the creative task of selectively selecting previously withheld information and pushing it rapidly and articulately out to the extraordinarily varied organizations that protect us, from local law enforcement, first responders, medical and emergency response teams, community leaders, utility industry managers with nuclear facilities, or farms of chemical and electrical storage tanks, mass transportation, and on and on.

Homeland security requires the vigilance of the many, rather than the control of the few. Awareness, prevention, protection, response and recovery are not hierarchical tasks delegated or dictated from the top.

The National Intelligence Reform Act of 2004 allowed—in that Congress took a major step to address these needs. It authorized broad central power for the new Director of National Intelligence and urged the DNI to create a tear-line report system, in which intelligence gathering by agencies is prepared so that information relating to intelligence sources and methods is easily severable within multi-layered products to allow wide sharing, while still protecting truly sensitive sources and methods from unauthorized disclosure.

The benefit of the protection to our communities lies on the other side of that tear-line. By concentrating on classification guidelines for protecting well-defined sources and methods and making refined decisions to protect that which really, truly require protection, more of the remaining information will be available for sharing with the public.

Your attention today follows a series of extraordinary efforts by this administration to control information with such severity and vengeance that it has blinded its constitutional partners here and in the judiciary. Most startling, this administration has used the information controls to institute policy and decision-making layers which have deemed even senior departmental officials from work-

ing—have doomed them to working in the sort of isolated stovepipes that are repeated again and again in the lessons of 9/11.

The practices that I have outlined in my prepared statement of DHS that have frustrated this effort can be read there. But I emphasize that it is DHS that is the place to start. By adopting legislative features, you can directly address your interests. Give DHS near-term objectives and extra resources to achieve results. Hold the Secretary of Homeland Security accountable for the mandates already contained in the law which dispensed such sweeping power.

The DNI has the authority to mandate DHS as a test-bed and to direct other departments and agencies to cooperate in changing the range of intelligence information controls. Hold the DNI accountable for regularly measuring achievements within the organizations under his control. Provide built-in monitoring by independent and experienced observers, such as Bill Leonard and the Information Security Oversight Office and Public Interest Declassification Board.

The tear-line system defined by Congress 4 years ago is the right standard. It is the place to start. It needs major attention to standardize guidance materials which can be applied with precision. Training and performance evaluation is necessary throughout.

But, most of all, demand and reward less information control in order to maximize communication. Translate the classification guides that Mr. Leonard referred to into action directives about what and how Congress—what and how should be communicated, rather than simply whether information might be classified and decontrolled. Hold Government officials and employees accountable for their decisions. When mistakes come to light, reeducate and retrain and emphasize the importance of the supervisors in that process.

Lastly, encourage the Office of the DNI and the full range of agencies under the DNI authority. This includes, not limited to DHS, to take careful cognizance of the well-established tradition of background briefings in which national security officials and the news media communicate informally in a manner meant to inform the public, including Congress and others in the executive, and provide a degree of confidence that secrecy is not being used to erode or impede civil liberties and free expression.

We would all do well to recall that our freedom has been protected and our homes have been secure because we as a people have understood how to best share information and how to best respond together to mutual threats. We look forward to cooperating with you in that effort.

Thank you.

Mr. CARNEY. Thank you, Mr. Armstrong.

[The statement of Mr. Armstrong follows:]

PREPARED STATEMENT OF SCOTT ARMSTRONG

JUNE 28, 2007

Chairwoman Harman, Ranking Member Reichert, and members of the Committee, thank you for this opportunity to address the issues of classification and pseudo-classification at the Department of Homeland Security.

My views today are my own, but I should note that I have been working closely with the Aspen Institute to sustain a six-year Dialogue between senior journalists, editors and publishers and high level US government officials from various national security and intelligence agencies, including senior members of congress and their staffs. The Dialogue on Journalism and National Security has attempted to address recurring concerns about the handling of sensitive national security information by government officials and representatives of the news media. The discussions have included the Attorney General, the Director of the Central Intelligence Agency and ranking officials from the National Security Council, the Department of Defense, the National Security Agency, the FBI as well as the CIA and the Department of Justice.

The Dialogue grew out of mutual concerns that legislation passed by both Houses of Congress in 2000 was, in effect, America's first Official Secrets Act. Although vetoed by President Clinton, the bill was reintroduced in 2001. In the wake of 9/11, high ranking officials of the national security community and the leadership of national press organizations recognized that the disclosure of sensitive national security information was a reason for concern. We found considerable agreement that legislation which inhibited virtually all exchanges of sensitive information—even responsible exchanges designed to increase public appreciation of national security issues—was not likely to make America more secure.

The goal, we seemed to agree, has been to have a well-informed citizenry that is assured of its safety without sacrificing its liberty. The lessons of 9/11 focused on sharing more information within government agencies, laterally across federal agency barriers and among federal, state, local governments and with critical private industries, community first responders and the public at large.

The Homeland Security Information Sharing Act, first passed by the House in 2002 and incorporated into the Homeland Security Act of 2004,¹ mandated the creation of a unique category of information known as "sensitive homeland security information." This category of SHSI information—as we have transliterated the acronym—was designed to permit the sharing of certain critical information with state and local authorities without having to classify it and require its recipients to hold clearances thus creating new barriers to communication. At the same time, SHSI designates information deemed necessary to withhold briefly from the general public while appropriate measures are taken to protect our communities.

The challenge for the Department of Homeland Security is not so much how to WITHHOLD secrets from the public and its local governmental representatives. The challenge is how to SHARE information so as to promote our security. For once government's first mission is not to silence "leaks," but to effectively share official information outside its usual restraints.

The discipline of controlling information needs to give way to the creative task of selecting previously withheld information and pushing it rapidly and articulately out to the extraordinarily varied organizations that protect us: local law enforcement; first responders; medical and emergency response teams; community leaders; utility industry managers with nuclear facilities or farms of chemical and energy storage tanks; mass transportation operators, and so forth.

Homeland security requires the vigilance of the many rather than the control of the few. Awareness, prevention, protection, response and recovery are not hierarchical tasks dictated from the top. Secrecy must yield to communication. This is no trivial task. The mission of information sharing is difficult enough within the cumbersome and slumbering giant newly merged from dozens of agencies and populated more than 180,000 employees. But that job is only the beginning since DIIS is the focal point for leveraging some 87,000 different governmental jurisdictions at the federal, state, and local level which have homeland security responsibilities involving tens of millions of Americans whose responsibilities cannot be choreographed from afar, but must be inspired by shared information.

In the National Intelligence Reform Act of 2004, the Congress took another major step to address this phenomenon. It authorized broad centralized power for the new Director of National Intelligence and urged the new DNI to create a tear line report system by which intelligence gathered by an agency is prepared so that the information relating to intelligence sources and methods is easily severable within multiple layered products to allow wide sharing while protecting truly sensitive sources and methods from unauthorized disclosure.

The benefit to the protection of our communities lies on the other side of that "tear line" system. By concentrating on the classification guidelines for protecting well defined sources and methods and making refined decisions to protect that which truly requires protection, more of the remaining information should be avail

¹ PL.107 296

able for sharing within the intelligence community as well as within the diversified and distributed elements of the colossus of those charged with Homeland Security responsibilities. The public benefits from these designations within internally published intelligence requiring protection because it makes majority of fact and analysis available for expedited release not just to homeland security organizations but also to the media and the public.

Your attention today follows a series of extraordinary efforts by this administration to control information with such severity and vengeance that it has blinded its constitutional partners here and in the judiciary. Most startling, this administration has used these information controls to institute policy and decision making layers which have doomed even senior departmental officials to work in the sort of isolated stovepipes described in the repetitious texts of 9/11 failures.

This is no longer a question of issues of over-classification but one of wholesale compartmentalized control and institutionalized intimidation through the use of draconian Non Disclosure Agreements. It appears designed more to inhibit and constipate internal communications in the federal government than to protect the national security.

Not surprisingly, the Department of Homeland Security wasted no time in replicating the move to Non Disclosure Agreements (NDA's). But it combined it with an effort to side step the congressional mandate to foster information sharing. Rather than educate the rest of the government on how to effectively communicate information, DHS dispersed new information control authority across the full spectrum of executive agencies. The uncoordinated proliferation of Sensitive But Unclassified designations —of the sort you address today already includes some remarkable missteps.

In one instance, the Department of Homeland Security drafted a draconian Non-Disclosure Agreement (NDA) designed to impose restrictions on tens of thousand federal employees and hundreds of thousands of state and local first responders. This NDA² for unclassified information more severe than the NDA's covering Sensitive Compartmented Information and even more sensitive information under the government's control.

This NDA required officials, employees, consultants and subcontractors to protect such "sensitive but unclassified information," which is defined as "an over arching term that covers any information. . . which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy [of] individuals . . . but which has **not** been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and **any other identifier used by other Government agencies** to categorize information as sensitive but unclassified."

This overbroad but legally binding requirement was implemented as a condition of access to certain unclassified information. Such an NDA represented a vast increase in government secrecy. It left control in the hands of an undefined and virtually unlimited number of supervisors. Those who signed the agreement were bound perpetually until it was explicitly removed. The NDA had no statutory authority and thus no defined criteria, rules, limitations or effective oversight. Although it did not provide an explicit rationale for withholding "Sensitive But Unclassified" information under the Freedom of Information Act, it surely provided an incentive to err in favor of using other exemptions to deny release.³

Although this NDA was withdrawn by DHS in January 2005, it was used last year at the Department to silence private Wackenhut guards who were speaking to the press about security breakdowns at the Department's Nebraska Avenue headquarters. Other instances of SBU constraints by government agencies, contractors and utilities appear to be used most often to discourage and prevent the public from participating in its government. Provisions similar to the DHS NDA have since appeared in other employee and contractor agreements both within DHS and within other departments.⁴

²DHS Form 11000 6 (08-04) "NON-DISCLOSURE AGREEMENT".

³See also DHS directive (MD 11042) on "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," dated May 11, 2004.

⁴See CRS Report RL33303, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, February 15, 2006 Genevieve J. Knezo, Specialist in Science and Technology Policy, Resources, Science, and Industry Division.

I repeat the details of DHS's failed practices to underline the suggestion that DHS is dramatically out of synch with its mandate to increase our security at home by aggressively—and yet carefully—sharing information in order to frustrate terrorists through prepared and coordinated responses of the most sophisticated intelligence capabilities on one hand, and our most formidable first line of defense—local law enforcement and first responders, on the other hand.

The Necessary Response

Adopt into legislation features which directly address your intentions.

1. **DHS is the right place to begin.** The current classification system within government is out of control and likely uncontrollable. Someone needs to start over with a new test bed. DHS, with its critically mission of communicating effectively across the federal government and with all other layers of state and local institutions has the greatest incentive for change.

2. **Give DHS near-term objectives** and extra resources to achieve concrete results. Hold the Secretary of Homeland Security accountable for the mandates contained in the law which dispensed such sweeping power.

3. **The DNI has the authority** to mandate DHS as a test-bed and to direct other departments and agencies to cooperate in changing the range of intelligence and information control systems. Hold the DNI accountable by regularly measuring achievements within organizations under his control.

4. **Provide built-in monitoring** by independent and experienced observers such as the **Information Security Oversight Office** and the **Public Interest Declassification Board** and provide the monitors with the resources to do their job.

5. **The tear-line system** designated by Congress four years ago is the right standard. It needs major attention to standardize guidance materials which can be applied with precision. All intelligence publication and sharing should be premised on carefully and formally defining sources and methods which require protection by isolating the smallest number of critical details. Information which requires less protection will receive greater circulation and earlier decontrol.

6. **Provide training and performance evaluation** incentives throughout all levels of DHS, in order to assure that the information which needs tight sources and methods control and only that information receives the ultimate protection.

7. **Create an electronic metadata tagging system** which requires that rigorous classification decision making will follow established guidance. Use it to assure that all levels understand they must conform with established practice and their effectiveness can and will be calibrated. Such a tagging system not only improves accountability, but also allows corrections and the protection of information improperly handled.

8. **Demand and reward less information control** in order to **maximize communication**.

Changing goals require reinforcement that **professionalizes** every level and every aspect of the information control process.

- Translate Information Control Guides (Classification Guides) into **action directives about what and how to communicate** rather than simply what and when information might be declassified or decontrolled.

- Provide opportunities for training and conceptual exercise which insist on communication up and down the line as well as lateral reviews and find mechanisms to make sure that the **communication runs to, as well as from, all intended recipients**.

9. **Hold government officials and employees accountable for their decisions**.

- When mistakes come to light, reeducate and retrain.
- Rethink the scope and purpose of both past practices and contemporary innovations by insisting *managers manage* the process with a willingness to keep changing procedures until they truly work.

- **Remove authority** from those who abuse it.
- Hold **supervisors responsible** by requiring them to assume **additional monitoring and training responsibilities** if those reporting to them fail to perform well-defined and specifically designated responsibilities. Similarly reward them when their aides perform their communication roles well.

- **End the incentive to classify** simply because over classifying has no consequences to individuals but information released can be career ending.

- Institute pro active audits and correlated retraining.

- Allow government employees and motivated citizens such as users of the FOIA to bring mistakes to light. Follow-up in a transparent manner to demonstrate that improved communication and improved information controls are

not necessarily on separate planes but are integrated concerns of all stake holders in a democracy.

10. Encourage the Office of the DNI and full range of Agencies under DNI authority including but not limited to DHS to take careful cognizance of the well established tradition of background briefings in which national security officials and the media communicate informally in a manner meant to inform the public (including the Congress and others in the Executive) and provide a degree of confidence that secrecy is not being used to erode or impede civil liberties and free expression.

- Include training for national security officials on responsible interaction with the news media by including the news media in the training
- Offer the media opportunities to learn about the laws, regulations and practices which involve secrecy and other national security protocols.

We would all do well to recall that our freedom has been protected and our homes have been secure because—as a people—we have understood how to best to share information and how best to respond together to mutual threats.

Mr. CARNEY. Ms. Spaulding for 5 minutes, please.

**STATEMENT OF SUZANNE E. SPAULDING, PRINCIPAL,
BINGHAM CONSULTING GROUP LLC**

Ms. SPAULDING. Thank you, Chair, ranking member and members of the committee. I very much appreciate this opportunity to be here today to testify about classification issues at the Department of Homeland Security. It is a very important issue, and I commend the committee for making it a priority.

In my 20 years working national security issues for the Government, I have seen firsthand how important it is to get this classification issue right. It may seem counterintuitive to some, but avoiding overclassification is essential to protecting vital national security secrets. Those handling classified documents will have greater respect for that Top Secret stamp if they know that things are only classified when their disclosure will truly harm national security.

When things are classified that clearly would not harm national security, it tempts some individuals to believe that they can decide what is really sensitive and what is not. Now let me be clear that, in making that observation, I am in no way trying to excuse the disclosure of classified information, merely to note that the risk of leaks I believe is heightened by overclassification.

A similar phenomenon follows the increasingly common practice of selective declassification by Government officials. Strategic and carefully considered decisions to make previously classified information available to the public can be important in increasing transparency. But when the disclosures appear to be designed to advance a particular political agenda or to gain an advantage in a policy dispute, it again undermines the respect for and confidence in the classification system. And this risk is heightened when the declassification is done selectively, so as to reveal only intelligence that supports one side of the issue, leaving contrary intelligence classified.

It is equally essential for our national security that information that can be shared without jeopardizing national security is not prevented by overclassification from getting to those who need it and could make use of it.

It is appropriate that the committee has decided to begin with an effort to make the Department of Homeland Security the gold

standard for reducing overclassification, because it is DHS that faces the most significant imperative to provide relevant information to a wide range of users, including those at the State and local level, the private sector, and even within DHS who are not traditional members of the national security community and are unlikely to hold security clearances. If information is unnecessarily restricted, it threatens homeland security by hampering the ability of these key players to contribute to the mission.

I know the committee is considering a number of ideas, a number of which have already been articulated here today, and I think these are very sound suggestions. There are additional near-term and longer-term steps that the committee might also consider.

One, require that intelligence documents be written in an unclassified version first to the maximum extent possible. Rather than creating a tear-line of unclassified or less sensitive information at the bottom of a document, why not set up the system so that no classified document can be prepared without first entering information into the unclassified section at the top of the document? This exercise could prompt a more careful effort to distinguish between truly classified information and that which can be shared more broadly and provide a visual reinforcement of the importance of writing in an unclassified form.

Two, enforce portion marking. This used to be the standard practice, where each paragraph was determined to be whether it was classified or unclassified. We have drifted away from that, and I think we should go back to really enforcing that requirement.

Three, use technology to tag information as it moves through the system. This provides even greater granularity than the paragraph portion marking, indicating which precise bits of information are classified. And then these tags, perhaps embedded in metadata, can move through the system with that information, facilitating the production of less classified documents.

Reverse the incentive to overclassify. This will not change until performance evaluations consider classification issues. It should be a specific factor when employees are evaluated for moving up or for raises. Employees who routinely overclassify should be held accountable and receive additional training, and employees should be rewarded for producing reports that can be widely disseminated.

Five, identify key Federal, State and local officials who can receive relevant classified information by virtue of their office, rather than by having to get a clearance. This is how we have always handled it for Members of Congress. More recently, we have included Governors; and DHS should consider extending it to other key officials.

And, six, develop innovative ways of sharing information without handing over documents; and I have got some specifics on that in my prepared testimony.

In conclusion, these are just a few ideas, based on practical experience working in the classified environments for nearly 2 decades. I know the committee is aware of the outstanding work of the Markle Foundation and others, and I recommend those to your consideration as well.

The problem of overclassification is an enduring one and presents a daunting challenge. The committee is to be commended for taking

up that challenge and endeavoring to set a new standard at DHS, and I appreciate the opportunity to contribute to that effort.

Thank you.

Mr. CARNEY. Thank you, Ms. Spaulding.

[The statement of Ms. Spaulding follows:]

PREPARED STATEMENT OF SUZANNE E. SPAULDING

JUNE 28, 2007

Chairwoman Harman, Ranking Member Reichert, and members of the Committee, thank you for this opportunity to testify today about classification issues at the Department of Homeland Security. This is an important issue and I commend the committee for making it a priority.

I was fortunate enough to spend 20 years working national security issues for the government, including 6 years at CIA and time at both the Senate and House Intelligence Committees. I have seen first hand how important it is to get the classification issue right.

It may seem counterintuitive to some, but avoiding over classification is essential to protecting vital national security secrets. Those handling classified documents will have greater respect for that "Top Secret" stamp if they know that things are only classified when their disclosure would truly harm national security. When things are classified whose disclosure clearly would not harm national security, it tempts some individuals to believe that they can decide what is really sensitive and what is not. This could apply to employees in the intelligence community or others, such as members of the media, who receive classified documents. In making this observation, I certainly do not mean in any way to excuse the disclosure of classified information, merely to note that the risk of leaks is heightened by over classification.

A similar phenomenon follows the increasingly common practice of "selective declassification" by government officials. This selective declassification can be accomplished either by unofficial leaks to the media or by official decisions to declassify material. Strategic and carefully considered decisions to make previously classified information available to the public can be an important and effective way of increasing the transparency that is so vital for a functioning democracy. However, when the disclosures appear to be designed to advance a particular political agenda or to gain advantage in a policy dispute, it again undermines the respect for and confidence in the classification system. An employee or reporter who sees senior officials deciding that classification isn't as important as their particular agenda may be emboldened to make similar decisions. This risk is heightened when the classification is done selectively so as to reveal only intelligence that supports one side of the issue, while leaving contrary intelligence classified.

Just as getting the classification process right is vital for protecting true secrets, it is essential that information that can be shared without jeopardizing national security is not prevented by over classification from getting to those who could make use of it. As the 9/11 Commission Report made clear, this is particularly urgent for our counterterrorism efforts.

It is appropriate that the Committee has decided to begin with an effort to make the Department of Homeland Security the "Gold Standard" for reducing over-classification, since DHS faces the most significant imperative to provide relevant information to, and receive and analyze information from, a wide range of users who are not traditional members of the national security community. Key players at the state and local level, in the private sector, and within DHS' own entities, are unlikely to have clearances. Yet they serve vital roles in protecting the homeland and can provide, benefit from, and help analysts to better understand, information that is gathered overseas and in the US. If this information is unnecessarily restricted, it threatens homeland security by hampering the ability of these key players to contribute to the mission.

I know that the committee is considering a number of ideas, including a certification process to ensure that those who have authority to classify documents are properly trained to recognize when information is truly sensitive and regular audits of existing classified documents to assess the scope and nature of any over classification. I think these are sound suggestions. There are additional near term and longer term steps that the Committee might also consider.

1. **Require that documents be written in unclassified version first, to the maximum extent possible.** Traditional practice in the intelligence community has been to prepare a classified document reflecting the intelligence and then, if dis

semination to non cleared individuals was required, to prepare an unclassified version at the bottom of the document after a "tear line." These are known as "tear sheets;" the recipient would tear off the bottom portion to provide to the un cleared recipient. Instead, to facilitate the admonition to move from a "need to know" to a "need to share" culture what the Markle Foundation called a "culture of distribution" why not set up the system so that no classified document can be prepared without first entering information in the unclassified section at the top of the document. There may be times when almost nothing can be put in the unclassified portion, but the exercise could prompt more careful effort to distinguish between truly classified information and that which can be shared more broadly. And putting the unclassified version at the top visually reinforces the shift in priorities.

2. Enforce "portion marking." It used to be standard practice that each paragraph of a document had to be individually determined and marked as classified or unclassified. This requires more careful consideration of what information is actually sensitive and assists in any later efforts to provide an unclassified version of the document. My sense is that, over time, documents are increasingly classified in their entirety, with no portion marking, making it far more difficult and cumbersome to "sanitize" the information for wider dissemination. A simple immediate step would be to enforce the requirement for portion marking for every classified document.

3. Use technology to tag information as it moves through the system. The optimum system would provide even greater granularity than the paragraph portion marking, indicating what precise bits of information are classified. These classification "tags" perhaps imbedded in metadata would then move with the information as it flows through the system and facilitate the preparation of unclassified versions of documents. The more precisely we can isolate truly sensitive information, the easier it will be to identify and disseminate unclassified information.

4. Reverse the "default" incentive to over-classify. Virtually all of the incentives today are in favor of over classification. The danger of not classifying information that is indeed damaging to national security is well understood. What is not as widely appreciated in the national security risk of over classification. Thus, there are effectively no penalties in the system for an individual decision to classify unnecessarily. This will not change until performance evaluations consider classification issues. Regular audits can provide insight into individual patterns as well as overall agency performance, for example. Employees who routinely over classify should be held accountable and receive additional training. And employees should be rewarded for producing reports that can be widely disseminated. In addition, the system should make it easy to produce unclassified documents and require a bit more effort to classify something. Requiring that unclassified documents be written first and enforcing the requirement for portion marking are some examples. Requiring that the specific harm to national security be articulated in each case might be another possibility, although it is important not to make the system so cumbersome that it undermines the ability to be quick and agile when necessary. Ultimately, you want a process that makes it harder to go around the system that to use it.

5. Identify key federal, state, and local officials who can receive relevant classified information by virtue of their office rather than having to get a clearance. This is how it has always worked with Members of Congress. More recently, this was adopted as the policy for governors. DHS should consider extending this to other key officials.

6. Develop innovative ways of sharing information without handing over documents. Ultimately, the key is to enhance understanding and knowledge. Too much emphasis is sometimes placed on sharing documents, rather than on sharing ideas, questions, and insights gleaned from those documents. This can often be done without revealing the sensitive information in the documents. In addition, when dealing with unclassified but sensitive information, such as business proprietary information, DHS could consider "partnership panels" where the government and business would come together in a neutral space, share information such as vulnerability assessments and threat information, so as to enhance mutual understanding and benefit from each others insights, but then leave the space without having handed over the documents.

These are just a few ideas based on practical experience working in classified environments for nearly two decades. I know that the Committee is aware of the outstanding work by the Markle Foundation and others in developing recommendations for improving information sharing and will take those under consideration as well.

The problem of over-classification is an enduring one and presents a daunting challenge. This Committee is to be commended for taking up that challenge and en

deavoring to set a new standard at DHS. I appreciate the opportunity to contribute to that important effort.

Mr. CARNEY. Mr. Agrast, please summarize for 5 minutes.

**STATEMENT OF MARK AGRAST, SENIOR FELLOW, CENTER
FOR AMERICAN PROGRESS**

Mr. AGRAST. Thank you, Mr. Carney.

My name is Mark Agrast. I am a Senior Fellow at the Center for American Progress, where I focus on civil liberties and national security concerns; and I previously spent a decade on Capitol Hill.

Most Americans understand and accept the need to protect Government information whose disclosure would endanger the Nation's security. But as the 9/11 Commission found, too much secrecy can put our Nation at greater risk, hindering oversight, accountability and information sharing, concealing vulnerabilities until it is too late to correct them, and undermining the credibility of the classification system itself.

Ten years ago, the Moynihan Commission concluded secrets could be protected more effectively if secrecy is reduced overall. Unfortunately, while the Clinton Administration made much headway in reducing unnecessary secrecy, today we are moving in the opposite direction. There were nearly three times as many classification actions in 2004 as in the last year of the Clinton Presidency; and while President Clinton declassified nearly a billion pages of historical material, the pace has slowed to a trickle in the last 6 years.

Today's epidemic of overclassification stems in part from rules that resolve all doubts in favor of nondisclosure and in part from standards so hard to administer that even skilled classifiers often get it wrong. Sometimes material is classified only to suppress embarrassing information.

Take the decision to classify the Taguba Report on prisoner abuse at Abu Ghraib. A reporter who had seen a copy of that report asked Secretary Rumsfeld why it was marked Secret. You would have to ask the classifier, Rumsfeld said. Or the decision to reclassify a 1950 intelligence estimate written only 12 days before Chinese forces entered Korea, predicting Chinese entry in the conflict was not probable.

Still, despite such failures, at least there are rules what can be classified, for how long and by whom. The same cannot be said for the designations used by Federal agencies to deny access to sensitive but unclassified information. Few of these pseudo-classifications have ever been authorized by Congress. They allow virtually any employee, and even private contractors, to withhold information that wouldn't even rate a Confidential stamp, with few standards or safeguards to prevent error and abuse.

As the Chair noted, last Sunday's Washington Post described a pseudo-classification scheme invented by the Vice President himself. His office has been giving reporters documents labeled treat as Top Secret/SCI, an apparent attempt to treat unclassified material as though it were Sensitive Compartmented Information, a special access designation reserved for secrets whose disclosure would cause exceptionally grave damage to national security.

I commend the committee, the subcommittee for its commitment to doing the oversight that is so long overdue; and I hope you won't

stop at oversight. It has been 10 years since the Moynihan Commission urged Congress to legislate the rules that protect national security information, rather than leaving it up to the executive branch to police itself. It is time for Congress to take up that challenge.

In some cases, this will require Government-wide solutions. For example, Congress could and should reinstate the presumption against classification in cases of significant doubt, the Clinton era policy which the Moynihan Commission urged Congress to codify.

Congress should also rein in the use of pseudo-classification, at a minimum prohibiting agencies from adopting unclassified designations that are not expressly authorized and mandating strict standards for any designations it does authorize to minimize their impact on public access.

Better still, Congress could refrain from authorizing unclassified designations in the first place. Such powers are all too easily given; and, once they are in place, it is virtually impossible to get rid of them.

Finally, Congress can take steps to reform the system one agency at a time by initiating reforms at the Department of Homeland Security. By making DHS the gold standard, Congress can promote best practices throughout the system.

My full statement includes recommendations to improve oversight of the classification system at DHS and to reduce the harmful effects of pseudo-classification as well. I would just review a couple of those in the half a minute or so that I have left.

I would recommend that Congress establish an independent DHS Classification Review Board to ensure that information is declassified as soon as it no longer meets the criteria for classification. Congress should establish an independent ombuds office within DHS to assist with declassification challenges and requests for declassification. It should require the DHS Inspector General to conduct periodic audits of the DHS classification program and report to Congress on the appropriateness of classification decisions. And it should require DHS to implement a system of certification for DHS officials with classification authority and to provide them with training and proper classification practices.

I would refer you to my testimony for recommendations regarding sensitive information controls.

I do think that by helping to ensure that the Government keeps secret only what needs to be kept secret, these measures and others would enhance both openness and security at DHS and throughout the Government.

Thank you.

[The statement of Mr. Agrast follows:]

PREPARED STATEMENT OF MARK D. AGRAST

JUNE 28, 2007

Madame Chair, Ranking Member Reichert, and members of the subcommittee, thank you for conducting this hearing and inviting me to testify.

My name is Mark Agrast. I am a Senior Fellow at the Center for American Progress, where I work on issues related to the Constitution, separation of powers, terrorism and civil liberties, and the rule of law.

Before joining the Center, I was an attorney in private practice and spent over a decade on Capitol Hill, most recently as Counsel and Legislative Director to Con

gressman William D. Delahunt of Massachusetts. A biographical statement is appended to my testimony.

In an address to the Oklahoma Press Association in February 1992, former Director of Central Intelligence, Robert M. Gates, now the Secretary of Defense, noted that the phrase "CIA openness" can seem as much an oxymoron as "government frugality" and "bureaucratic efficiency."

That seeming contradiction in terms illustrates the anomalous role that secrecy plays in a democracy that depends so profoundly on an informed and engaged citizenry.

At the same time, most Americans understand and accept the need to withhold from public view certain national security information whose disclosure poses a genuine risk of harm to the security of the nation.

But the events of 9/11 taught us how dangerously naïve it would be to equate secrecy with security. As the 9/11 Commission conclude, too much secrecy can put our nation at greater risk, hindering oversight, accountability, and information sharing.

Too much secrecy—whether through over classification or through pseudo-classification—conceals our vulnerabilities until it is too late to correct them.

It slows the development of the scientific and technical knowledge we need to understand threats to our security and respond to them effectively.

It short circuits public debate, eroding confidence in the actions of the government.

And finally, it undermines the credibility of the classification system itself, encouraging leaks and breeding cynicism about legitimate restrictions. As Associate Justice Potter Stewart famously cautioned in the Pentagon Papers case:

I should suppose that moral, political, and practical considerations would dictate that a very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.¹

The Commission on Protecting and Reducing Government Secrecy, chaired by Sen. Daniel Patrick Moynihan, reached a similar conclusion in its 1997 report: "The best way to ensure that secrecy is respected, and that the most important secrets *remain* secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall."²

Classification, Declassification and Reclassification

The Moynihan Commission was created by Congress to consider whether it was time to rethink the vast system of secrecy that had been brought into being during the Cold War. The Commission recommended a series of statutory reforms to the classification system that were widely praised but never implemented.

The spirit of the Moynihan recommendations can certainly be discerned in the contemporaneous amendments to the classification system that were instituted by President Clinton under Exec. Order No. 12958. The order established a presumption of access, directing that "If there is significant doubt about the need to classify information, it shall not be classified." Similarly, the order provided that "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level." The Clinton order also:

- Limited the duration of classification, providing that where the classifier cannot establish a specific point at which declassification should occur, the material will be declassified after 10 years unless the classification is extended for successive 10 year periods under prescribed procedures.
- Provided for automatic declassification of government records that are more than two years old and have been determined by the Archivist of the United States to have permanent historical value, allowing for the continued classification of certain materials under specified procedures.
- Established a balancing test for declassification decisions in "exceptional cases," permitting senior agency officials to exercise discretion to declassify information where "the need to protect such information may be outweighed by the public interest in disclosure of the information."
- Prohibited reclassification of material that had been declassified and released to the public under proper authority.

¹ N.Y. Times Co. v. U.S., 403 U.S. 713, 729 (1971) (Stewart, J., concurring).

² REPORT OF THE COMM'N ON PROTECTING & REDUCING GOV'T SECRECY (1997) at xxi [hereinafter Moynihan Commission Report].

- Authorized agency employees to bring challenges to the classification status of information they believe to be improperly classified.
- Created an Interagency Security Classification Appeals Panel (ISCAP) to adjudicate challenges to classification and requests for mandatory declassification, and to review decisions to exempt information from automatic declassification.

The changes instituted by President Clinton were largely erased by his successor, who issued a revised executive order in 2003. Exec. Order No. 13292 eliminated the presumption of access, leaving officials free to classify information in cases of "significant doubt." It also:

- Relaxed the limitations on the duration of classification, and made it easier for the period to be extended for unlimited periods.
- Postponed the automatic declassification of protected records 25 or more years old from April 2003 to December 2006, and reduced the showing that agencies must make to exempt historical records from automatic declassification.
- Revived the ability of agency heads to reclassify previously declassified information if the information "may reasonably be recovered."
- Allowed the Director of Central Intelligence to override decisions by ISCAP, subject only to presidential review.

The results of this shift in policy are reflected in the annual classification statistics published by the Information Security Oversight Office (ISOO). The number of classification actions by the government hit an all time high of 15.6 million in 2004, with only slightly fewer (14.2 million) reported in 2005. This was nearly twice the number of classification actions (8.6 million) taken in 2001, the first year of the Bush administration, and three times the number (5.8 million) taken in 1996, the last year of President Clinton's second term.³

As classification actions have soared, declassification actions have plummeted. President Clinton oversaw the declassification of more historic materials than all previous presidents combined. During his last six years in office, 864 million pages were declassified, hitting an all-time high of 204 million pages in 1997 alone. Under the Bush administration, the numbers have fallen precipitously. Only 245 million pages were declassified from 2001–2005, with fewer than 30 million pages were declassified in 2005.⁴

Apart from its costs to both openness and security, all this classifying and declassifying comes at a heavy financial cost as well. In 2005, the cost of securing classified information was \$7.7 billion, of which only \$57 million was spent on declassification. In all, for every dollar the federal government spent to release old secrets, it spent \$134 to create new ones.⁵

What the numbers cannot reveal is whether classification decisions are lawful and appropriate. Estimates of the extent of over classification vary, but I was particularly struck by Mr. Leonard's testimony before this subcommittee last March, in which he said that an audit conducted by the Information Security Oversight Office found that even trained classifiers, armed with the most up to date guidance, "got it clearly right only 64 percent of the time."⁶

There are also instances in which over classification is the result, not of honest error, but of a desire to conceal. Both the Clinton and Bush executive orders prohibit the use of the classification system to "conceal violations of law, inefficiency, or administrative error" or prevent embarrassment to a person, organization, or agency." Yet at least some recent classification decisions could have had little purpose other than to suppress information that might be embarrassing to the government.

A particularly troubling example is the decision by the Department of Defense to classify in its entirety the March 2004 report of the investigation by Maj. Gen. Antonio M. Taguba of alleged abuse of prisoners by members of the 800th Military Police Brigade at Baghdad's Abu Ghraib Prison. According to an investigation by the Minority Staff of the House Committee on Government Reform:

One reporter who had reviewed a widely disseminated copy of the report raised the issue in a Defense Department briefing with General Peter Pace, the Vice Chairman of the Joint Chiefs of Staff, and Secretary Rumsfeld. The reporter noted that 'there's clearly nothing in there that's inherently secret, such as intelligence sources and methods or troop movements' and asked: 'Was this kept

³INFO. SEC. OVERSIGHT OFFICE, NAT'L ARCHIVES & RECORDS ADMIN., REPORT TO THE PRESIDENT 2005 at 13.

⁴*Id.* at 15.

⁵OPENTHEGOVERNMENT.ORG, SECRECY REPORT CARD 2006 at 4.

⁶*Overclassification and Pseudo-classification: The Impact on Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Comm. on Homeland Sec., 110th Cong. (2007) (statement of J. William Leonard).*

secret because it would be embarrassing to the world, particularly the Arab world?" General Pace responded that he did not know why the document was marked secret. When asked whether he could say why the report was classified, Secretary Rumsfeld answered: "No, you'd have to ask the classifier."⁷

The desire to prevent embarrassment seems also to have played a role in the Bush administration's aggressive reclassification campaign. According to a February 2006 report by the National Security Archive, the administration has reclassified and withdrawn from public access 9,500 documents totaling 55,500 pages, including some that are over 50 years old. For example:

- complaint from the Director of Central Intelligence to the State Department about the bad publicity the CIA was receiving after its failure to predict anti-American riots in Colombia in 1948.
- A document regarding an unsanctioned CIA psychological warfare program to drop propaganda leaflets into Eastern Europe by hot air balloon that was canceled after the State Department objected to the program.
- A document from spring 1949, revealing that the U.S. intelligence community's knowledge of Soviet nuclear weapons research and development activities was so poor that America and Britain were completely surprised when the Russians exploded their first atomic bomb six months later.
- A 1950 intelligence estimate, written only 12 days before Chinese forces entered Korea, predicting that Chinese intervention in the conflict was "not probable."⁸

These reclassification actions call to mind the observations of the late Erwin N. Griswold, former Solicitor General of the United States and Dean of Harvard Law School, who argued the Pentagon Papers case before the Supreme Court in 1971. Presenting the case for the government, he had argued that the release of the Pentagon Papers would gravely damage the national security. Nearly two decades later, Griswold reflected on the lessons of that case:

It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another. There may be some basis for short term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past. This is the lesson of the Pentagon Papers experience, and it may be relevant now.⁹

Pseudo-Classification

For all its faults, the classification system has many virtues as well. Classification actions are subject to uniform legal standards pursuant to executive order. These actions can be taken by a limited number of officials who receive training in the standards to be applied; they are of limited duration and extent; they are monitored by a federal oversight office; they can be challenged; and they can be appealed.

The same cannot be said for the potpourri of unclassified control markings used by federal agencies to manage access to sensitive government information, most of which are defined by neither statute nor executive order, and which collectively have come to be known pejoratively as the "pseudo-classification" system.

Among the better known are Sensitive But Unclassified (SBU), Sensitive Security Information (SSI), Sensitive Homeland Security Information (SHSI), Critical Infrastructure Information (CII), Law Enforcement Sensitive (LES), and For Official Use Only (FOUO).

While some of these control markings are authorized by statute,¹⁰ others have been conjured out of thin air. Some of these pseudo-classification regimes allow virtually any agency employee (and often private contractors) to withhold information without justification or review, without any time limit, and with few, if any, internal controls to ensure that the markings are not misapplied.

A March 2006 report by the Government Accountability Office (GAO) found that the 26 federal agencies surveyed use 56 different information control markings (16

⁷MINORITY STAFF OF HOUSE COMM. ON THE JUDICIARY, 107TH CONG., REPORT ON SECRECY IN THE BUSH ADMINISTRATION (2004) at 50.

⁸MATTHEW M. AID, NAT'L SEC. ARCHIVE, DECLASSIFICATION IN REVERSE: THE U.S. INTELLIGENCE COMMUNITY'S SECRET HISTORICAL DOCUMENT RECLASSIFICATION PROGRAM (2006).

⁹Erwin N. Griswold, *Secrets Not Worth Keeping: The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25.

¹⁰See, e.g., Aviation and Transp. Sec. Act, Pub. L. No. 107-71; Fed. Info. Sec. Act, Pub. L. No. 107-347; Homeland Sec. Act, Pub. L. No. 107-296; Critical Infrastructure Info. Act, Pub. L. No. 107-296.

of which belong to one agency) to protect sensitive unclassified national security information. The GAO also found that the agencies use widely divergent definitions of the same controls.¹¹

According to the GAO report, the Department of Homeland Security (DHS) employs five of these control markings: For Official Use Only (FOUO) (agency wide); Law Enforcement Sensitive (LES) (agency-wide); Limited Official Use (LOU) (U.S. Secret Service); Protected Critical Infrastructure Information (PCII) (Directorate for Preparedness); and Sensitive Security Information (SSI) (Transportation Security Administration and U.S. Coast Guard).

The department's approach to the use of these designations is set forth in a DHS management directive regarding the treatment of sensitive but unclassified information originating within the agency.¹² The directive is chiefly concerned with the For Official Use Only designation, which it says will be used "to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation." The directive identifies 11 categories of SBU information that can be designated as FOUO, and provides that the designation can be made by any DHS employee, detailee, or contractor and will remain in effect indefinitely until the originator or a management official determines otherwise.

For good measure, the directive notes that where other agencies and international organizations use similar terminology but apply different requirements to the safe guarding of the information, the information should be treated in accordance with whichever requirements are the more restrictive.

A 2004 report by the JASON Program Office at MITRE Corporation suggests that the designation authorities at DHS are not atypical: "Sensitive but unclassified" data is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used."¹³

As in the case of classification and reclassification actions, these designations have at times been used not to protect legitimate national security secrets, but to spare the government from embarrassment. In a March 2005 letter to Rep. Christopher Shays, then the Chairman of the House Committee on Government Reform, Rep. Henry Waxman cited examples in which:

- The State Department withheld unclassified conclusions by the agency's Inspector General that the CIA was involved in preparing a grossly inaccurate global terrorism report.
- The State Department concealed unclassified information about the role of John Bolton, Under Secretary of State for Arms Control, in the creation of a fact sheet that falsely claimed that Iraq sought uranium from Niger.
- The Department of Homeland Security concealed the unclassified identity and contact information of a newly appointed TSA ombudsman whose responsibility it was to interact daily with members of the public regarding airport security measures.
- The CIA intervened to block the chief U.S. weapons inspector Charles A. Duelfer, from revealing the unclassified identities of U.S. companies that conducted business with Saddam Hussein under the Oil for Food program.
- The Nuclear Regulatory Commission sought to prevent a nongovernmental watchdog group from making public criticisms of its nuclear power plant security efforts based on unclassified sources.¹⁴

In another case, currently in litigation, a federal air marshal blew the whistle when TSA attempted to reduce security on "high risk" flights, and the agency allegedly retaliated by retroactively designating the material he had disclosed as Sensitive Security Information (SSI).¹⁵

Another concern arises out of the interplay between unclassified control markings and the Freedom of Information Act (FOIA). Certain unclassified control markings, including Sensitive Security Information (SSI) and Critical Infrastructure Informa-

¹¹ U.S. GOV'T ACCOUNTABILITY OFFICE, REP. NO. GAO 06 385, INFORMATION SHARING: THE FEDERAL GOVERNMENT NEEDS TO ESTABLISH POLICIES AND PROCESSES FOR SHARING TERRORISM-RELATED AND SENSITIVE BUT UNCLASSIFIED INFORMATION (2006).

¹² Safeguarding Sensitive But Unclassified (For Official Use Only) Information, Mgt. Dir. No. 11042 (2004), at http://www.fas.org/sgp/othergov/dhs_sbu.html, revised by Mgt. Dir. No. 11042.1, (2005), at http://www.fas.org/sgp/othergov/dhs_sbu_rev.pdf [hereinafter Safeguarding].

¹³ JASON PROGRAM OFFICE MITRE CORPORATION, HORIZONTAL INTEGRATION: BROADER ACCESS MODELS FOR REALIZING INFORMATION DOMINANCE 5 (2004).

¹⁴ H.R. Rep. No. 109 8, at 16 (2005) (letter from Henry Waxman to Christopher Shays).

¹⁵ PROJECT ON GOV'T OVERSIGHT, ALERT: ROBERT MACLEAN v. DHS (2007), at <http://pogo.org/p/government/rmaclean-dhs.html>

tion (CII), are specifically exempt by statute from release under FOIA. But some agencies have claimed that other unclassified control markings constitute an independent legal basis for exempting information from public disclosure under FOIA even in the absence of an express statutory exemption and even where the information does not fit within an existing exemption.

Such claims prompted the American Bar Association's House of Delegates to adopt a resolution in February 2006 urging the Attorney General to clarify that such designations should not be used to withhold from the public information that is not authorized to be withheld by statute or executive order.

As it happens, the DHS directive meets the ABA standard. It provides that FOUO information is not automatically exempt from disclosure under FOIA and that FOUO information may be shared with other agencies and government entities "provided a specific need to know has been established and the information is shared in furtherance of a coordinated and official governmental activity."¹⁶

But whether or not an agency has a legal basis for withholding pseudo classified information not otherwise exempt under FOIA is almost beside the point. The designation is itself sufficient to exert a chilling effect on FOIA disclosures. As Thomas S. Blanton of the National Security Archive testified before a subcommittee of the House Committee on Government Reform in March 2005, "the new secrecy stamps tell government bureaucrats 'don't risk it'; in every case, the new labels signal 'find a reason to withhold.'"¹⁷

An article published in the Washington Post on June 24, 2007, brought to light a pseudo-classification scheme apparently invented by the Vice President of the United States. His office has been giving reporters documents labeled: "Treated As: Top Secret/SCI" an apparent attempt to treat unclassified material as though it were Sensitive Compartmented Information (SCI)—a special access designation reserved for secrets whose disclosure would cause 'exceptionally grave damage to national security.'"¹⁸

Unlike the Cheney innovation, Special Access Programs (SAPs), which limit access above and beyond the three tiered classification system, are authorized by law, and are confined to a relatively limited circle of senior officials. Exec. Order No. 12859, as amended, provides that unless otherwise authorized by the President, only certain named officials are authorized to establish such programs. The list includes the Secretaries of State, Defense, and Energy, and the DCI, or the principal deputy of each. Interestingly, the list does not include the Vice President—perhaps in anticipation of his novel assertion that the Office of the Vice President is not an agency of the Executive Branch and need not comply with the requirement under Exec. Order 12859 that such agencies file an annual report with ISOO.¹⁹

The fact that SAPs are authorized by executive order does not mean they are immune from the deficiencies of pseudo-classifications. The Moynihan Commission noted a "lack of standardized security procedures" that "contributes to high costs and other difficulties," and recommended the establishment of a single set of security standards for Special Access Programs—another of its sensible recommendations which, as far as is known, has not been carried out.²⁰

Recommendations for Congress

Madame Chair, you and the subcommittee should be commended for exercising your oversight authority over the treatment of national security information—both classified and unclassified—at the Department of Homeland Security. Such scrutiny is essential, and it is long overdue.

I would also respectfully suggest that the time has come for the committee, and for Congress, to exercise its *legislative* authority over these matters. For 67 years, Congress has largely ceded that authority to the president, and as I hope I have explained, the results have been decidedly mixed.

It has been ten years since the Moynihan Commission urged Congress to legislate the rules that protect national security information, rather than leaving it up to the executive branch to police itself. It is time for Congress to take up that challenge.

A. Systemic solutions

¹⁶ Safeguarding, *supra* note 11.

¹⁷ *Emerging Threats: Over-classification and Pseudo-classification: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats and Int'l Relations of the House Comm. on Gov't Re form*, 109th Cong. (2005) (statement of Thomas S. Blanton).

¹⁸ Barton Gellman & Jo Becker, *A Different Understanding with the President*, WASH. POST, June 24, 2007, at A1.

¹⁹ Peter Baker, *Cheney Defiant on Classified Material: Executive Order Ignored Since 2003*, WASH. POST, June 22, 2007, at A1.

²⁰ Moynihan Commission Report at 28.

Many of the problems facing the classification system are systemic, and they require comprehensive, government-wide solutions. Among other things, Congress should reinstate the provisions of Exec. Order No. 12958 which (a) established a presumption against classification in cases of significant doubt (a policy which the Moynihan Commission urged Congress to codify); (b) permitted senior agency officials to exercise discretion to declassify information in exceptional cases where the need to protect the information is outweighed by the public interest in disclosure; and (c) prohibited reclassification of material that had been declassified and released to the public under proper authority.

Congress also should undertake a thorough and comprehensive examination of the growing use of agency control markings to restrict access to unclassified information. Much has been said, and rightly so, about the importance of information sharing among government agencies. But what is the justification for a system that entrusts low-level employees and private contractors with the non-reviewable discretion to determine whether an unclassified document—a document that doesn't even rate a "Confidential" stamp—a document that may not even qualify for a FOIA exemption—is too sensitive for public view?

Before Congress acquiesces in the further proliferation of these designations, it should consider whether those that already exist place an unwarranted burden on the free exchange of information, not only among government officials, but between the government and the people who elect it.

At a minimum, Congress should prohibit agencies from adopting unclassified controls that are not expressly authorized by statute (or executive order), and should mandate strict standards for any controls it does authorize to minimize their impact on public access.

H.R. 5112, the Executive Branch Reform Act, which was reported by the House Government Reform Committee during the 109th Congress, directs the Archivist of the United States to promulgate regulations banning the use of information control designations not defined by statute or executive order. If the Archivist determines that there is a need for some agencies to use such designations "to safeguard information prior to review for disclosure," the regulations shall establish standards designed to minimize restrictions on public access to information. The regulations shall be the sole authority for the use of such designations, other than authority granted by statute or executive order.

This approach would ameliorate some of the worst features of what is today an unregulated wilderness of inconsistent standards and insufficient checks. But it begs the question of whether Congress should be authorizing agency officials to withhold unclassified information in the first place. Such powers are all too easily given, and once they are in place, it is virtually impossible to get rid of them.

I hope that Congress will consider codifying standards that incorporate these policies. But there are also many steps that can be taken to reform the management of national security information one department at a time. By undertaking such reforms at the Department of Homeland Security—by making DHS the "gold standard"—Congress can create a model for best practices that other agencies can adopt.

B. The Classification System at DHS

(1) Congress should establish an Information Security Oversight Office, modeled after the Information Security Oversight Office at the National Archives and Records Administration, to oversee security classification programs at DHS. Its responsibilities would include development of implementing directives and instructions; maintenance of liaison with ISOO and agency counterparts; monitoring of agency compliance and preparation of reports to Congress; and development of security classification education and training programs.

(2) Congress should establish an independent DHS Classification Review Board to ensure that information is declassified as soon as it no longer meets the criteria for classification. Among the responsibilities of the board would be to facilitate and review requests for declassification and classification challenges, and to conduct an independent ongoing review of classified materials to determine whether they are properly classified.

(3) Congress should establish an independent ombuds office within DHS to provide assistance with classification challenges and requests for declassification.

(4) Congress should require the DHS Inspector General to conduct periodic audits of the DHS classification program and report to Congress on the appropriateness of classification decisions.

(5) Congress should require DHS to implement a system of certification for DHS officials with classification authority and to provide them with training in proper classification practices.

C. Sensitive Information Controls at DHS

As noted above, I hope that Congress will reconsider the question of whether agency employees and private contractors should be given a license to withhold unclassified, non FOIA exempt information from the public. But short of curtailing the use of unclassified control markings, there are steps that can be taken by DHS to minimize error and abuse, and reduce the impact of pseudo-classification on public access to information.

- (1) Congress should require DHS to place strict limits on the number of agency officials authorized to designate FOUO and other unclassified information as controlled, to implement a system of certification for DHS officials with designation authority, and to provide authorized officials with training in proper designation practices.
- (2) Congress should require DHS to limit the duration of controls on unclassified information and provide procedures by which such controls can be removed.
- (3) Congress should require DHS to develop procedures by which members of the public can challenge unclassified designations.
- (4) Congress should require the DHS Inspector General to conduct periodic audits of the use of controls on unclassified information and report to Congress on the appropriateness of designations.
- (5) The Homeland Security Committee should oversee DHS implementation of—
 - a. The directives regarding the use of the SSI designation by TSA which Congress included in the DHS Appropriations Bill for FY 2007 (Pub. L. 109–295). Those directives require review of any document designated SSI whose release is requested and require release of certain documents designated SSI after three years unless the DHS Secretary provides an explanation as to why it should not be released.
 - b. The recommendations included in the GAO report of June 2005 evaluating the use of the SSI designation by TSA.²¹ The GAO found significant deficiencies in TSA's management of SSI, and recommended that the Secretary of DHS direct the TSA Administrator to:
 - i. Establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI.
 - ii. Establish clear responsibility for the identification and designation of information that warrants SSI protection.
 - iii. Establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA.
 - iv. Establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.

Conclusion

By helping to ensure that the government keeps secret only the information that needs to be secret, these measures would enhance both openness and security at DHS and throughout the government.

Thank you.

Mr. CARNEY. Well, I thank the witnesses for their testimony; and I remind each member he or she will have 5 minutes to question the panel.

I now recognize myself for 5 minutes, and this is for all the witnesses. If you could do one thing to overcome the overclassification or pseudo-classification problem at DHS, what reform initiative or best practice would you adopt? I know Mr. Agrast, you just mentioned a few, but Mr. Leonard and Mr. Armstrong, Ms. Spaulding?

Mr. LEONARD. One that I would recommend, some agencies, such as State and CIA, as a best practice have independent advisory commissions comprised of historians that advise those agencies on the effectiveness of their agencies' declassification program. There is no reason why such an advisory committee could not be established on the front end of the process. An advisory committee may

²¹ U.S. GOV'T ACCOUNTABILITY OFFICE, REP. NO. GAO-05-677 TRANSPORTATION SECURITY ADMINISTRATION: CLEAR POLICIES AND OVERSIGHT NEEDED FOR DESIGNATION OF SENSITIVE SECURITY INFORMATION (2005).

be of the principal consumers, State and local officials with appropriate clearances who could provide advice back to the Department as to the effectiveness of what they are classifying and its impact on their information needs.

Mr. ARMSTRONG. Mr. Carney, I would emphasize—I think Ms. Spaulding made reference to the same phenomenon—in the tear-line system, or something like the tear-line system, emphasize the communication of important information in the least—controlled manner necessary. Remember that the purpose of all communication in Government, whether it is the most sensitive intelligence or not, is to influence someone somewhere to take cognizance of it and to change their behavior or focus their analytical skills. In doing so, put the emphasis on communication and then minimize and restrict the sources and methods portion of the communication to protect it. But put the emphasis on communicating, not withholding.

Ms. SPAULDING. I think the most important thing is to do something to begin to change the culture and the mindset, and I think that is set at the top. That is a tone and an emphasis that is set at the top.

So I would consider issuing, maybe even from the President, an Executive Order, for example, that would direct the agencies, Department of Homeland Security to begin with, to include in their performance evaluations the issue of overclassification and underclassification, how employees do in terms of getting the classification right, that that would be a factor in how they are evaluated. I think that would go a long way in setting the right tone.

Mr. CARNEY. Are the evaluators in your opinion able to do that? Don't they have a vested interest in kind of keeping the system as it is?

Ms. SPAULDING. Well, I think it would be combined with the kinds of recommendations that have been made at this table, including regular audits of documents that have been classified; and that would help to inform those kinds of performance appraisals as to whether this employee regularly is found to have overclassified documents, for example, or whether this employee has written a great number of unclassified reports that have been able to be widely disseminated.

Those performance appraisals are fairly standardized actions; and if those forms have a specific thing that you have to fill in that relates to how this employee does in terms of their classification decisions, I think that would provide an appropriate incentive.

Mr. LEONARD. If I could add to that, as a follow-on, another best practice that is very closely related to that, the CIA, even though it is not required at the national level, requires a personal identifier on every product they produced as to who was responsible for the classification decision; and something like that facilitates a follow-up and holding people accountable.

Mr. AGRAS. If I could also add, I completely agree with the recommendations, particularly with the remarks of Ms. Spaulding.

Mr. Reichert opened his portion of the hearing by talking about his experience as a law enforcement officer at the State and local level. I think there are two kind of prosecutors. There are two kinds of law enforcement officers. There is the kind that says my

job is to convict as many people as possible, and there is the other kind who says my job is to get the truth, and I will be satisfied that I have done my job if I convict the people who are guilty and don't convict the people who are not guilty.

I think that is the cultural change that has to happen at these agencies so the premium is set not solely on the number of documents you have successfully kept from the public but using discernment and using fine judgment in determining when and whether classification decisions should be made.

Mr. CARNEY. Thank you.

Mr. Leonard, I know your office is responsible for regulating classification by agencies within the executive branch; and you consistently stated that the Government classifies too much information. Why is this happening, in your opinion? What is the reason?

Mr. LEONARD. Reasons are varied, but I would agree more than anything else with Ms. Spaulding's assessment that it is really one of culture. We are very effective in terms of holding people accountable for the inappropriate disclosure of information, either administratively or criminally. Very rarely, if ever, have I ever seen anyone held accountable for inappropriately withholding or hoarding information.

Mr. CARNEY. Too many people have classification power?

Mr. LEONARD. Yes.

Another best practice—and Mr. Agrast mentioned this—is DOE follows it. They actually require people to be trained and certified before they can affix classification controls on the product, as opposed to just having clearance and having access to it.

So something along those lines would facilitate accountability, because you could have something to take away from them now if they abuse it, and it restricts the universe of people that you have to make sure are appropriately trained. So there is a lot of benefits to it all around.

Mr. CARNEY. Thank you.

I now recognize the ranking member, my good friend from Washington, Mr. Reichert.

Mr. REICHERT. Thank you, Mr. Chairman.

I just wanted to go back to Mr. Carney's original question, which was if you do one thing. I want to ask it in just a little bit of a different way.

What is the biggest hurdle—I have an answer in my mind, in my experience, but what is the biggest hurdle to overcome in this whole issue of not sharing information and overclassifying?

Okay, I will give you a hint at least where I am going with this. Somebody mentioned the stovepipe thing. And, to me, really to get more specific, governance, who has control over the information? Who is the lead person? At the local level in the sheriff's office, with 38 police departments and the sheriffs in the county, you know, the battle is over who controls the server that has the information. And you are running into that sort of an issue at the Federal level. I am sure you are.

Mr. ARMSTRONG. I think what we have seen, Mr. Reichert, is that the leadership of the various departments—that we had the merger into the Department of Homeland Security and specific incentives given—direction given to the DNI to begin to break down

the barriers, break down the stovepipes. But it requires the leadership to do that.

The drift in the bureaucracy is toward safety, is toward the norm, is toward withholding, is toward not exposing oneself to criticism. Until and unless someone initiates a test-bed of a new direction and puts the incentive on making sure that everyone knows what they need to know, but all of what they need to know, this will not happen. Things will not change. It will default back to the old system. I think that is the problem we are faced with.

Mr. REICHERT. Certainly the difficulty is highlighted as you bring the 22 departments under the one Homeland Security umbrella. But it even gets more complicated then as you reach outside to the other agencies that don't report to the homeland security effort. So I mean it is a huge issue to overcome. Does anyone have any suggestions?

Mr. LEONARD. I would suggest, Mr. Reichert, another major hurdle is the myriad of information protection regimes that exist within the Federal Government. There is no individual who can comprehend and understand all of them, even know of all of them. While there are efforts under way within the executive branch to streamline that and what have you, there are still contributing issues, many of them statutorily based, in terms of establishing requirements for protecting critical infrastructure information and things along those lines. What that results in is it is incomprehensible to me how an operator, who has decisions to make on a day-to-day basis and getting information from multiple sources, how they can even begin to understand what they can and what they can't disclose. And it can result in paralysis.

Mr. REICHERT. It almost seems as though the local agencies take the lead in this arena. As we in Seattle took a look at the LInX System spearheaded by the U.S. attorney's office, the FBI choosing not to participate in that information-sharing experiment and the U.S. Naval Intelligence then taking the lead with the U.S. attorney's office, finally after a few years we have a system in Seattle now that we have partners.

I think one team at a time, one maybe part of the country at a time coming together, being able to showcase a success, would you not agree that might be a way to address this issue? Mr. Agrast?

Mr. AGRAST. Yes, I very strongly agree. I think pilot programs and State experimentation is really a very useful tool here. When people, as you have heard, are reluctant to change, I think they need to see success stories. They need to see that it can work and that there is a better way to do these things.

Mr. REICHERT. Ms. Spaulding, you mentioned along the same lines this cultural change, and several of you have. I really see that as really the biggest issue, and it is a leadership concern, you know, from protecting to sharing. Do you have any ideas on how to really jump-start that?

Ms. SPAULDING. Well, the Markle Foundation talks about creating a culture of distribution. But I think you are right. That is the most important thing. And, as I said, I think there are some suggestions in terms of creating—there is already, as Mr. Leonard pointed out, a huge incentive for classifying documents. It is career ending if you fail to classify something that is then disclosed and

causes harm to national security. So there is a huge incentive to classify. It is much easier to classify a document. It is just a safe bet. And we have to create incentives for being more careful about that decision and incentives for creating unclassified documents. You know, as I said, I have got a number of suggestions for that in my testimony.

But I do think there are legitimate concerns that present a stumbling block. You asked about what are some of the major stumbling blocks. Having the trust that an agency isn't going to take your information and somehow disrupt your operational activity, and I am sure you understand exactly what I am talking about.

Mr. REICHERT. Yes, I do.

Ms. SPAULDING. And it is a legitimate concern, but it is also one of the major reasons why we find problems sharing information, particularly among law enforcement and, you know, agencies that have the ability to take action or are undertaking operations. And I saw this in spades when I was at the intelligence, when I was at CIA, and their relationships with the other agencies, FBI, Customs, whatever, the concerns on both sides of that that one or the other would take the information and run an operation that would mess up what the other agency had going.

So the challenge there, the solution there it seems to me has got to be operational coordination. It can't be that you are allowed to withhold that information, and there I think is a place where particularly State and locals can provide excellent models.

Mr. REICHERT. Those agencies that have ongoing investigations, especially with CIs, are very concerned about sharing information. My time has expired. Mr. Chairman, I yield back.

Mr. CARNEY. Thank you, Mr. Reichert.

I will now recognize Mr. Dent from Pennsylvania for 5 minutes, and we will probably do another round. Okay.

Mr. DENT. Thank you, Mr. Chairman.

Ms. Spaulding, you just brought up an issue that I find interesting, and I wonder if we could talk about this issue. There are incentives to overclassify right now, but the only real control over information resides in the classification realm. Isn't overclassification a natural reaction to unauthorized disclosure of sensitive but unclassified materials? There is no punishment for—serious punishment for releasing sensitive material.

Ms. SPAULDING. As I said in my testimony, I think that overclassification actually contributes to a lack of respect for the classification mark and therefore actually makes it harder to protect true national security secrets.

I think overclassification is a detriment to protecting truly secret information. So I do think that that is also part of the incentive structure in terms of when you are looking at leaks is that overclassification does contribute to that kind of culture as well.

I think in addition to clearly trying to find ways to identify people who disclose classified information and take action, firm action against people who disclose classified information, I think it is important also at all levels of Government to reinforce the respect for classification markings.

Mr. DENT. Well, I guess as a follow-up, how can the Federal Government really balance the need? You know, how do we balance

this need I guess to share information on the one hand, and at this unclassified level, with the knowledge that somebody somewhere continues to leak sensitive but unclassified information? I think that is really the crux of the problem here.

Ms. SPAULDING. My sense is that trying to hold more tightly to that information within those stovepipes has not been an effective way of preventing those disclosures. And therefore, I think, as I said, in addition to trying to use technology to help us with audit trails to keep track of who is accessing information, who is printing information, who has access to the information that might be disclosed and trying to identify those people and hold them accountable, that it really is important that we indicate that we have taken more care in labeling things. So that when they are labeled, whether it is classified or sensitive, law enforcement sensitive, that in fact there has been a reasoned determination that could be upheld as we look at it after the fact that this would harm national security or homeland security or law enforcement interests.

Mr. ARMSTRONG. Mr. Dent?

Mr. DENT. Yes.

Mr. ARMSTRONG. After three decades as a journalist in this town, I have to recognize that there is an information economy, there is an information currency within secrecy, that every major agency at every senior level leaks classified information, controls and manipulates classified information, and in parallel at other levels, either in other agencies or in the same agencies, other people speak candidly, but they speak in terms of things that aren't genuinely secret.

When everything is secret, as Potter Stewart said, nothing is secret. No one knows what to respect. Most senior officials have some criteria, make judgments every day, several times a day, about how to share information that is technically classified but to get it out in some form that it believes the public needs to know or their colleagues need to know, without filing all the forms. It has caused problems from time to time, but there is an ongoing communication about what those standards are. And it is possible, particularly in the form that we are talking about today, to emphasize how to communicate without damaging the national security. Better to do it within the system than have it done without the system.

Mr. DENT. I guess you are addressing it, but the question I have, how do we balance this need to share this information at the unclassified level with the knowledge that somebody somewhere continues to leak sensitive but unclassified information? I guess that is the question. How do you balance this?

Mr. AGRAS. Mr. Dent, one thing I guess I would hope we would do is have these unclassified markings regulated by Congress. They have taken on a life of their own. They are so numerous and so varied, there are so few standards and safeguards. You know, the classification system, with all its problems, looks pretty good compared to the pseudo-classification nonsystem.

So rather than have agencies making ad hoc decisions and bringing the entire system of controlled information into disrepute, shouldn't Congress take a look at this comprehensively and decide whether such categories should exist at all? Or whether, instead,

if information is truly in need of safeguarding, it ought not to be classified in the first place?

Mr. DENT. Yield back.

Mr. CARNEY. Thank you, Mr. Dent.

We will start a second round of questions here.

Mr. Armstrong, in your estimation, how effective has DHS been in producing reports and products at the unclassified level?

Mr. ARMSTRONG. Well, we read unclassified material when it is presented by DHS. But, more often, we read the relevant information when it is put in unclassified form when it is leaked to DHS because of the form of controls that have been established that effectively discourage and inhibit candid communication. The number of inappropriate things that have happened to try and block contractors or the employees of contractors in using information in labor disputes, for example, does not increase respect for the system; and the difficulty we have had is the difficulty of accountability.

Mr. Leonard administers some degree of accountability within a classified system, but it is very difficult to do when, effectively, a department has authority to create all sorts of constraints on communication that are not necessarily constraints designed to protect national security; and the farther we move away from those for the original purpose to protect sources and methods, to protect short-term objectives that need to be accomplished, to coordinate at different levels of our government, and we move into areas where political control and sensitivity—it seems to us on the outside that the Secretary of Homeland Security has been virtually unaccountable to Congress, unaccountable to other agencies and ineffective in the administration of his mandates.

Mr. CARNEY. What is the solution to that?

Mr. ARMSTRONG. Well, I don't know what you need to do to get him here to talk with you, but I think there are issues that can be addressed about in a public executive session. He has unbelievably large sets of responsibilities, but at various levels throughout the Department there are professionals who would like to do their job properly. I don't believe that they are getting the leadership. The leadership sometimes emerges when it is variegated by questions.

The truth—the most important purpose, Woodrow Wilson said, for Congress is not to pass legislation but to inquire into how government is effectively being done; and it is that process that needs to occur and occur more publicly.

Mr. CARNEY. Thank you.

Mr. Agrast, in your estimation, how much information is being withheld by DHS and its private contractors that is unclassified and non-FOIA exempt?

Mr. AGRAST. I actually have no idea how much is being withheld. We have indications that, to the extent there are standards, they aren't being followed. I will give you one example, if I may, from my prepared testimony.

The GAO, the Government Accountability Office, issued a report in June of 2005 evaluating the use of the SSI designation by the TSA, which is of course a unit of the Department; and they found significant deficiencies in TSA's management of SSI information

and recommended that the Secretary direct the Administrator to take a number of remedial actions.

One is to establish clear guidance and procedures for using the regulations to determine what constitutes SSI. The second is to establish clear responsibility for the identification and designation of information that warrants SSI protection. The third was to establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies and procedures governing the designation process and to communicate that responsibility throughout TSA. And, finally, to establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.

Clearly, those recommendations have yet to be implemented in a proper way; and it is surely within the purview of this subcommittee to inquire as to the progress that is or is not being made.

Mr. CARNEY. How should DHS implement the new control of unclassified information originating from CUI that Ambassador McNamara developed? Mr. Agrast, sorry to interrupt your drink there.

Mr. AGRAST. You know, I would have to give more consideration to how they ought to go about it on an agency basis. Certainly there are some of these areas that are interdepartmental in nature, and some of these kinds of policies and practices require coordination. I am not sure that a single agency can do it.

Mr. CARNEY. So you don't think it is something that DHS could do quickly or necessarily?

Mr. AGRAST. Not sure.

Mr. CARNEY. Ms. Spaulding, do you have any idea?

Ms. SPAULDING. Certainly one thing to consider, and particularly when you are talking about these pseudo-classifications, is requiring that they be done at a fairly senior level. Mr. Leonard touched on this both with respect to classification and pseudo-classification, having people well-trained and certified with the authority to, you know, put that stamp on the document. But particularly in this area I think it would be helpful to move those decisions to a more senior level.

Mr. CARNEY. Thank you.

Mr. Reichert, any more questions?

Mr. REICHERT. Thank you. I will just make mine pretty quick here.

Last year, we passed a bill that directed some cooperation in fighting terrorism, cooperating at the international level, mostly through technology, those countries like Israel and Canada and the U.K. and others who have been—Australia—who have been kind of dealing with this a little longer than we have, a lot longer in some cases. They have developed some technologies and some systems. Would you consider that we should consult these countries who have had this experience in classifying and unclassifying and over-classification and pseudo—classification? Should we be looking for leadership from those other countries? And do you have any information or knowledge about that occurring now? Anybody.

Mr. LEONARD. I don't have any knowledge, direct knowledge in terms of whether it is occurring or not, Mr. Reichert. But something along those lines, that definitely has merit, if only from the perspective of ensuring that we have congruous systems. Because I know that we do that on the classification level where we routinely, especially with our close allies and friendly nations, work to ensure that we have congruous systems that facilitate the sharing of classified information, especially when we are in a coalition environment and things along those lines. So those types of efforts clearly could bear fruit on the unclassified level.

Now to the extent of whether they are occurring or not, I really don't know.

Mr. REICHERT. Anyone else have—

Mr. ARMSTRONG. Most of the technologies that I think to which you are referring that would be helpful here are employed in the business realm already and for different reasons and with different levels, obviously, of security and devotion to principles. But we are talking about techniques. The notion of embedding metadata begins to track intellectual product and the ability to not only determine where it has gone or how it has been used or whether it has been appropriately dealt with but also to automatically begin to alert people to the fact that it is no longer controlled or it requires additional controls for an additional reason.

All of those things are present at high levels in certain business environments, but they are expensive, and the incentives have to be high. Capitalism tends to find some degree of incentives. One would think that homeland security and anti-terrorism measures could find at least as high a level.

Mr. REICHERT. Mr. Agrast, did you have—

Mr. AGRAST. Congressman, I think it is an extraordinarily thoughtful question. There has been a tendency not to look abroad for answers, and I think that has demonstrated itself to be a mistake. We don't have to do what other countries do, but we should at least learn what we can from them.

Mr. REICHERT. Yes. Thank you.

One last thought. With this new world of technology and our soldiers fighting around the world and their access to various communication devices, cell phones and cameras in their cell phones and computers, they are communicating back to their families and friends real-time info on battles occurring or briefings that are occurring. How do you see that issue being addressed in the sharing of information that could be critical to our operations in fighting terrorism?

Mr. LEONARD. Well, what I see that is emblematic of a challenge we always have, and that is we are playing catch-up to technology all the time, especially from the point of, A, leveraging it but, B, understanding the ramifications from a security or vulnerability point of view as well. And then when we attempt to address it, we usually do it in a hand-fisted way, which is sometimes analogous to trying to repeal gravity.

So the challenge is to somehow, some way get in front of that curve all the time and fully understand the capabilities and the limitations of the technology and try to keep our policies abreast

of it, rather than being in that proverbial catch-up mode which we seem to be in.

Ms. SPAULDING. I don't think there is a technological solution, whether it is some new technology or shutting down some of those technology outlets, because you will never get them all. I think the only solution to that particular issue is training. I mean, you have simply got to sensitize, you know, those folks to what they can and should not be sharing and disclosing publicly. And you will never have perfect success with that, but it seems to me that trying to attack that, the basis of technology, is not going to be very successful.

Mr. REICHERT. Yeah. You know—one of the experiences I will share real quick—in the Green River investigation in 1987, the search warrant to be served on the suspect who we finally arrested years, years later—we had a meeting on the service of the search warrant. I was the detective in charge of the search of this subject's house; and, as I arrived, standing on the front porch was a reporter from our local newspaper to greet me. So someone within the meeting immediately shared the information.

That is really one of the frustrations I think in this whole thing. You talked about building trust and in those local agencies and within those agencies within the Federal Government, too, in having the knowledge that their information is protected as the investigation is ongoing. The firewalls that can be built in a system to protect that information is a huge hurdle I think to overcome and also plays into the cultural change.

So I appreciate you being here this morning, and thank you so much for your testimony.

Mr. CARNEY. Well, I want to thank the witnesses as well for their invaluable testimony. This truly is an issue that we have to further explore to shed light on the classification issue. It is absolutely essential.

The members of the subcommittee will probably have additional questions for the witnesses, and we ask that you respond expeditiously in writing.

Hearing no further business, the subcommittee stands adjourned. [Whereupon, at 11:15 a.m., the subcommittee was adjourned.]

FOR THE RECORD

PREPARED OPENING STATEMENT OF THE HONORABLE JANE HARMAN, CHAIRMAN,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK
ASSESSMENT

MARCH 22, 2007

- Good morning. I'd like to welcome you all to this hearing on the increasing problems of over classification and pseudo classification and their impact on what is the lifeblood of our homeland security: effective information sharing with our State, local, and tribal law enforcement officers.

- The United States has had a classification regime in place for decades: information and intelligence typically falls into one of three categories: Top Secret, Secret, or Confidential.

- Our nation adopted this regime for one reason: to protect sensitive sources and methods.

- Contrary to the practice of some in the federal Intelligence Community, classified markings are NOT to be used to protect political turf or to hide embarrassing facts from public view.

- Indeed, a recurrent theme throughout the 9/11 Commission's report was the need to prevent widespread over classification by the Federal government. The Commission found that over classification interferes with sharing critical information and impedes efficient responses to threats.
- The numbers tell us that we are still not heeding the Commission's warning.
- Eight million new classification actions in 2001 jumped to 14 million new actions in 2005, while the quantity of declassified pages dropped from 100 million in 2001 to 29 million in 2005.
- In fact, some agencies were recently discovered to be withdrawing archived records from public access and reclassifying them!
- Expense is also a problem: \$4.5 billion spent on classification in 2001 increased to \$7.1 billion in 2004, while declassification costs fell from \$232 million in 2001 to \$48.3 million in 2004.
- In addition, an increasing number of policies to protect sensitive but unclassified information from a range of Federal agencies and departments has begun to have a dramatic impact.
- At the Federal level, over 28 distinct policies for the protection of this information exist.
- Unlike classified records, moreover, there is no monitoring of or reporting on the use or impact of protective sensitive unclassified information markings.
- The proliferation of these pseudo-classifications is interfering with interagency information sharing, increasing the cost of information security and limiting public access.
- Case in point: this document from the Department of Homeland Security (HOLD UP RADICALIZATION IN THE STATE OF CALIFORNIA SURVEY).
- In a few weeks, I will be leading a field hearing to Torrance, California, to examine the issues of domestic radicalization and "home grown" terrorism.
- This DHS document a survey on radicalization in the State of California is marked "Unclassified/For Official Use Only."
- On Page 1 in a footnote, the survey states that it cannot be released "to the public, the media, or other personnel who do not have a valid 'need to know' without prior approval of an authorized DHS official."
- Staff requested and was denied that approval.
- Staff also asked for a redacted version of the document so we could use at least some of its contents at the coming California hearing. DHS was unable to provide one.
- Let me be clear: I'm not denying that there may be sensitive information included in this survey, but it illustrates my point: what good is unclassified information about threats to the homeland if we can't discuss at least some of it at a hearing?
- How can we expect DHS and others to engage the public on important issues like domestic radicalization if we hide the ball?
- Unfortunately, this is nothing new. In 1997, the Moynihan Commission stated that the proliferation of these new designations are often mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information.
- These continuing trends are an obstacle to information sharing across the Federal government and with State, local, and tribal partners including most especially with our partners in the law enforcement community.
- Unless and until we have a robust intelligence and information sharing system in place in this country, with a clear and understandable system of classification, we will be unable to prevent a terrorist attack on the scale of 9/11 or greater.
- That is why this Subcommittee will focus its efforts in the 110th Congress on improving information sharing with our first preventers the men and women of State, local, and tribal law enforcement who are the "eyes and ears" on our front lines.
- And it's why we will pay particular attention to the issues of over-classification and pseudo-classification of intelligence and what we can do to ensure that we err on the side of sharing information.
- We'll do this work in the right way partnering with our friends in the privacy and civil liberties community who want to protect America while preserving our cherished rights.
- I would like to extend a warm welcome to our witnesses who will be talking about these issues.
- On our first panel, we have assembled an array of experts who will be testifying about the extent of these problems and where things are trending.

- Our second panel of law enforcement leaders will talk about how over-classification and pseudo-classification are impacting their ability to keep our communities safe.
- In addition, I hope the witnesses will provide the Subcommittee with a sense of how we might solve the challenges ahead of us, with the goal of ensuring the flow of information between the Federal government and State, local and tribal governments.
- Welcome to you all.

PREPARED STATEMENT OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY

MARCH 22, 2008

- Thank you, Madame Chair, and I join you in welcoming our distinguished witnesses today to this important hearing on the problem of over and pseudo classification of intelligence.
- Information sharing between the Federal government and its State, local and tribal partners is critical to making America safer.
- But we won't get there if all we have is more and more classification, and more and more security clearances for people who need access to that classified information.
- The focus should be different.
- The Federal government instead must do all it can to produce intelligence products that are unclassified.
- Unclassified intelligence information is what our nation's police officers, first responders, and private sector partners need most.
- They have told me time and time again that what they DON'T need is information about intelligence sources and methods.
- An officer on patrol in Jackson, Mississippi, or Des Moines, Iowa, has no use for the name of the person in Afghanistan, Africa, or elsewhere who provided the information or whether it was obtained from an intercepted communication.
- What he or she wants to know is if the information is accurate, reliable and timely.
- If so, police chiefs and sheriffs can use it to drive their daily operations especially when it comes to deciding where to put their people to help prevent attacks.
- That's what intelligence is all about: if it can't tell an officer on the beat what to prepare for and how, what good is it?
- Over-classification and pseudo classification are nothing new, but 9/11 has made these problems worse.
- It's my understanding that security concerns after the September 11th attacks prompted some agencies and departments to shield whole new categories of information with Confidential, Secret or Top Secret markings.
- What might have started as a noble intention to protect the homeland has broken down into a system of often excessive, abusive and/or politically motivated classification decisions.
- It's time to fix things.
- This hearing will be the first of several on over and pseudo classification and will help us get a handle on the scope of the problem.
- I hope each of the witnesses will be forthcoming in their assessments of these issues and how we can help.
- Welcome to you all. I look forward to your testimony.

